NATIONAL CREDIT UNION ADMINISTRATION

RULES AND REGULATIONS

TRANSMITTAL SHEET **CHANGE 4**

NCUA 8006 (M3500) DATE: November 2005

TO: THE BOARD OF DIRECTORS OF THE FEDERAL CREDIT UNION OR THE FEDERALLY INSURED CREDIT UNION ADDRESSED:

This is Change 4 to the National Credit Union Administration Rules and Regulations (Revised April 2004).

1. **PURPOSE.** To update the April 2004 edition of the National Credit Union Administration Rules and Regulations in the following manner:

   a. **Part 701—Organization and Operation of Federal Credit Unions.**

   § 701.21—Loans to members and lines of credit to members. Revised paragraphs (e), (f), and (g)(1).

   b. **Part 717—Fair Credit Reporting.**

   Subpart A—General Provisions.

   § 717.1—Purpose. New.

   § 717.2—Examples. New.

   § 717.3—Definitions. Revised paragraphs (a) and (b); (d); (i); (k) and (l).

   Subpart D—Medical Information. New.

   § 717.30—Obtaining or using medical information in connection with a determination of eligibility for credit. New.

   § 717.31—Limits on redisclosure of information. New.

   § 717.32—Sharing medical information with affiliates. New.

   c. **Part 748—Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance.**

   § 748.0—Security Program. Revised paragraph (b).

   Appendix B to Part 748—Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice. Added new Appendix B.

2. This revision also corrects typing and printing errors.
3. **INSTRUCTIONS:**
   a. Your April 2004 NCUA Rules and Regulations should be updated as follows:

REMOVE OLD PAGES	INSERT NEW PAGES
i–xv	i–xv
701–7 thru 701–10	701–7 thru 701–10
708a–3 thru 708a–4	708a–3 thru 708a–4
717–1 thru 717–2	717–1 thru 717–7
748–1 thru 748–2	748–1 thru 748–2
748–5 thru 748–6	748–5 thru 748–9
792–5 thru 792–8	792–5 thru 792–8
Index–1 thru Index–4	Index–1 thru Index–4

4. **PREAMBLES.** Enclosed with Change 4 are Federal Register published preambles. Although not part of the rules, you may find them useful for explanatory purposes.

TABLE OF CONTENTS

*THESE PARTS APPLY TO FEDERALLY INSURED STATE-CHARTERED CREDIT UNIONS AS WELL AS FEDERAL CREDIT UNIONS

TABLE OF CONTENTS

Section *Page*

*THESE PARTS APPLY TO FEDERALLY INSURED STATE-CHARTERED CREDIT UNIONS AS WELL AS FEDERAL CREDIT UNIONS

TABLE OF CONTENTS

*THESE PARTS APPLY TO FEDERALLY INSURED STATE-CHARTERED CREDIT UNIONS AS WELL AS FEDERAL CREDIT UNIONS

TABLE OF CONTENTS

Section *Page*

*THESE PARTS APPLY TO FEDERALLY INSURED STATE-CHARTERED CREDIT UNIONS AS WELL AS FEDERAL CREDIT UNIONS

TABLE OF CONTENTS

*THESE PARTS APPLY TO FEDERALLY INSURED STATE-CHARTERED CREDIT UNIONS AS WELL AS FEDERAL CREDIT UNIONS

TABLE OF CONTENTS

*THESE PARTS APPLY TO FEDERALLY INSURED STATE-CHARTERED CREDIT UNIONS AS WELL AS FEDERAL CREDIT UNIONS

TABLE OF CONTENTS

TABLE OF CONTENTS

*THESE PARTS APPLY TO FEDERALLY INSURED STATE-CHARTERED CREDIT UNIONS AS WELL AS FEDERAL CREDIT UNIONS

TABLE OF CONTENTS

*THESE PARTS APPLY TO FEDERALLY INSURED STATE-CHARTERED CREDIT UNIONS AS WELL AS FEDERAL CREDIT UNIONS

TABLE OF CONTENTS

Section *Page*

Part 745—Share Insurance and Appendix*

Subpart A—Clarification and Definition of Account Insurance Coverage

Subpart B—Payment of Share Insurance and Appeals

Part 747—Administrative Actions, Adjudicative Hearings, Rules of Practice and Procedure, and Investigations*

Subpart A—Uniform Rules of Practice and Procedure

*THESE PARTS APPLY TO FEDERALLY INSURED STATE-CHARTERED CREDIT UNIONS AS WELL AS FEDERAL CREDIT UNIONS

TABLE OF CONTENTS

TABLE OF CONTENTS

Section *Page*

TABLE OF CONTENTS

Section *Page*

*THESE PARTS APPLY TO FEDERALLY INSURED STATE-CHARTERED CREDIT UNIONS AS WELL AS FEDERAL CREDIT UNIONS

TABLE OF CONTENTS

Section *Page*

Subpart C—Public Observation of NCUA Board Meetings Under the Sunshine Act

Part 792—Requests for Information Under the Freedom of Information Act and Privacy Act, and by Subpoena; Security Procedures for Classified Information

Subpart A—The Freedom of Information Act

TABLE OF CONTENTS

Section *Page*

TABLE OF CONTENTS

Section *Page*

(6) *Early payment.* A member may repay a loan, or outstanding balance on a line of credit, prior to maturity in whole or in part on any business day without penalty.

(7) *Loan interest rates—*

(i) *General.* Except when a higher maximum rate is provided for in paragraph (c)(7)(ii) of this section, a Federal credit union may extend credit to its members at rates not to exceed 15 percent per year on the unpaid balance inclusive of all finance charges. Variable rates are permitted on the condition that the effective rate over the term of the loan (or line of credit) does not exceed the maximum permissible rate.

(ii) *Temporary rates.—(A) 21 percent maximum rate.* Effective from December 3, 1980 through May 14, 1987, a Federal credit union may extend credit to its members at rates not to exceed 21 percent per year on the unpaid balance inclusive of all finance charges. Loans and line of credit balances existing on or before May 14, 1987, may continue to bear rates of interest of up to 21 percent per year after May 14, 1987.

(B) *18 percent maximum rate.* Effective May 15, 1987, a Federal credit union may extend credit to its members at rates not to exceed 18 percent per year on the unpaid balance inclusive of all finance charges.

(C) *Expiration.* After September 8, 2006, or as otherwise ordered by the NCUA Board, the maximum rate on federal credit union extensions of credit to members shall revert to 15 percent per year. Higher rates may, however, be charged, in accordance with paragraph (c)(7)(ii)(A) and (B) of this section, on loans and line of credit balance existing on or before September 8, 2006.

(8)(i) Except as otherwise provided herein, no official or employee of a Federal credit union, or immediate family member of an official or employee of a Federal credit union, may receive, directly or indirectly, any commission, fee, or other compensation in connection with any loan made by the credit union.

(ii) For the purposes of this section:

Compensation includes non monetary items, except those of nominal value.

Immediate family member means a spouse or other family member living in the same household.

Loan includes line of credit.

Official means any member of the board of directors or a volunteer committee.

Person means an individual or an organization.

Senior management employee means the credit union's chief executive officer (typically, this individual holds the title of President or Treasurer/Manager), any assistant chief executive officers (e.g., Assistant President, Vice President, or Assistant Treasurer/Manager), and the chief financial officer (Comptroller).

Volunteer official means an official of a credit union who does not receive compensation from the credit union solely for his or her service as an official.

(iii) This section does not prohibit:

(A) Payment, by a Federal credit union, of salary to employees;

(B) Payment, by a Federal credit union, of an incentive or bonus to an employee based on the credit union's overall financial performance;

(C) Payment, by a Federal credit union, of an incentive or bonus to an employee, other than a senior management employee, in connection with a loan or loans made by the credit union, provided that the board of directors of the credit union establishes written policies and internal controls in connection with such incentive or bonus and monitors compliance with such policies and controls at least annually.

(D) Receipt of compensation from a person outside a Federal credit union by a volunteer official or non senior management employee of the credit union, or an immediate family member of a volunteer official or employee of the credit union, for a service or activity performed outside the credit union, provided that no referral has been made by the credit union or the official, employee, or family member.

(d) *Loans and Lines of Credit to Officials—*

(1) *Purpose.* Sections 107(5)(A) (iv) and (v) of the Act require the approval of the board of directors of the Federal credit union in any case where the aggregate of loans to an official and loans on which that official serves as endorser or guarantor exceeds $20,000 plus pledged shares. This paragraph implements the requirement by establishing procedures for determining whether board of directors' approval is required. The section also prohibits preferential treatment of officials.

(2) *Official.* An "official" is any member of the board of directors, credit committee or supervisory committee.

(3) *Initial approval.* All applications for loan or lines of credit on which an official will be

either a direct obligor or an endorser, cosigner or guarantor shall be initially acted upon by either the board of directors, the credit committee or loan officer, as specified in the Federal credit union's bylaws.

(4) *Board of directors' review.* The board of directors shall, in any case, review and approve or deny an application on which an official is a direct obligor, or endorser, cosigner or guarantor if the following computation produces a total in excess of $20,000:

(i) Add:

(A) The amount of the current application.

(B) The outstanding balances of loans including the used portion of an approved line of credit, extended to or endorsed, cosigned or guaranteed by the official.

(C) The total unused portion of approved lines of credit extended to or endorsed, cosigned or guaranteed by the official.

(ii) From the above total subtract:

(A) the amount of shares pledged by the official on loans or lines of credit extended to or endorsed, cosigned or guaranteed by the official.

(B) The amount of shares to be pledged by the official on the loan or line of credit applied for.

(5) *Nonpreferential treatment.* The rates, terms and conditions on any loan or line of credit either made to, or endorsed or guaranteed by

(i) an official

(ii) an immediate family member of an official, or

(iii) any individual having a common ownership, investment or other pecuniary interest in a business enterprise with an official or with an immediate family member of an official shall not be more favorable than the rates, terms and conditions for comparable loans or lines of credit to other credit union members. "Immediate family members" means a spouse or other family member living in the same household.

(e) *Insured, Guaranteed and Advance Commitment Loans.* A loan secured, in full or in part, by the insurance or guarantee of, or with an advance commitment to purchase the loan, in full or in part, by the Federal Government, a State government or any agency of either, may be made for the maturity and under the terms and conditions, including rate of interest, specified in the law, regulations or program under which the insurance, guarantee or commitment is provided.

(f) *20-Year Loans.* (1) Notwithstanding the general 12-year maturity limit on loans to members, a federal credit union may make loans with maturities of up to 20 years in the case of:

(i) a loan to finance the purchase of a mobile home if the mobile home will be used as the member-borrower's residence and the loan is secured by a first lien on the mobile home, and the mobile home meets the requirements for the home mortgage interest deduction under the Internal Revenue Code,

(ii) a second mortgage loan (or a nonpurchase money first mortgage loan in the case of a residence on which there is no existing first mortgage) if the loan is secured by a residential dwelling which is the residence of the member-borrower, and

(iii) a loan to finance the repair, alteration, or improvement of a residential dwelling which is the residence of the member-borrower.

(2) For purposes of this paragraph (f), mobile home may include a recreational vehicle, house trailer or boat.

(g) *Long-Term Mortgage Loans:*

(1) *Authority.* A federal credit union may make residential real estate loans to members, including loans secured by manufactured homes permanently affixed to the land, with maturities of up to 40 years, or such longer period as may be permitted by the NCUA Board on a case-by-case basis, subject to the conditions of this paragraph (g).

(2) *Statutory limits.* The loan shall be made on a one- to four-family dwelling that is or will be the principal residence of the member-borrower and the loan shall be secured by a perfected first lien in favor of the credit union on such dwelling (or a perfected first security interest in the case of either a residential cooperative or a leasehold or ground rent estate).

(3) *Loan application.* The loan application shall be a completed standard Federal Housing Administration, Veterans Administration, Federal Home Loan Mortgage Corporation, Federal National Mortgage Association or Federal Home Loan Mortgage Corporation/Federal National Mortgage Association application form. In lieu of use of a standard application the Federal credit union may have a current attorney's opinion on file stating that the forms in use meet the requirements of applicable Federal, state and local laws.

(4) *Security instrument and note.* The security instrument and note shall be executed on

the most current version of the FHA, VA, FHLMC, FNMA, or FHLMC/FNMA Uniform Instruments for the jurisdiction in which the property is located. No prepayment penalty shall be allowed, although a Federal credit union may require that any partial prepayments be made on the date monthly installments are due and be in the amount of that part of one or more monthly installments that would be applicable to principal. In lieu of use of a standard security instrument and note, the Federal credit union may have a current attorney's opinion on file stating that the security instrument and note in use meet the requirements of applicable Federal, state and local laws.

(5) *First lien, territorial limits.* The loan shall be secured by a perfected first lien or first security interest in favor of the credit union supported by a properly executed and recorded security instrument. No loan shall be secured by a residence located outside the United States of America, its territories and possessions, or the Commonwealth of Puerto Rico.

(6) *Due-on-sale clauses:*

(i) Except as otherwise provided herein, the exercise of a due-on-sale clause by a Federal credit union is governed exclusively by Section 341 of Public Law 97–320 and by any regulations issued by the Federal Home Loan Bank Board implementing Section 341.

(ii) In the case of a contract involving a long-term (greater than twelve years), fixed rate first mortgage loan which was made or assumed, including a transfer of the liened property subject to the loan, during the period beginning on the date a state adopted a constitutional provision or statute prohibiting the exercise of due-on-sale clauses, or the date on which the highest court of such state has rendered a decision (or if the highest court has not so decided, the date on which the next highest court has rendered a decision resulting in a final judgment if such decision applies statewide) prohibiting such exercise, and ending on October 15, 1982, a Federal credit union may exercise a due-on-sale clause in the case of a transfer which occurs on or after November 18, 1982, unless exercise of the due-on-sale clause would be based on any of the following:

(A) the creation of a lien or other encumbrance subordinate to the lender's security instrument which does not relate to a transfer of rights of occupancy in the property;

(B) the creation of a purchase money security interest for household appliances;

(C) a transfer by devise, descent, or operation of law on the death of a joint tenant or tenant by the entirety;

(D) the granting of a leasehold interest of 3 years or less not containing an option to purchase;

(E) a transfer to a relative resulting from the death of a borrower;

(F) a transfer where the spouse or children of the borrower become an owner of the property;

(G) a transfer resulting from a decree of a dissolution of marriage, a legal separation agreement, or from an incidental property settlement agreement, by which the spouse of the borrower becomes an owner of the property;

(H) a transfer into an inter vivos trust in which the borrower is and remains a beneficiary and which does not relate to a transfer of rights of occupancy in the property; or

(I) any other transfer or disposition described in regulations promulgated by the Federal Home Loan Bank Board.

(7) *Assumption of real estate loans by nonmembers.* A federal credit union may permit a nonmember to assume a member's mortgage loan in conjunction with the nonmember's purchase of the member's principal residence, provided that the nonmember assumes only the remaining unpaid balance of the loan, the terms of the loan remain unchanged, and there is no extension of the original maturity date specified in the loan agreement with the member. An assumption is impermissible if the original loan was made with the intent of having a nonmember assume the loan.

(h) *Removed and replaced by part 723.*

(i) *Put Option Purchases in Managing Increased Interest-Rate Risk for Real Estate Loans Produced for Sale on the Secondary Market.*

(1) *Definitions.* For purposes of this § 701.21(i):

(i) "Financial options contact" means an agreement to make or take delivery of a standardized financial instrument upon demand by the holder of the contract at any time prior to the expiration date specified in the agreement, under terms and conditions established either by (A) a contract market designated for trading such contracts by the Commodity Futures Trading Commission, or (B) by a Federal credit union and a primary dealer in

Government securities that are counterparties in an over-the-counter transaction.

(ii) "FHLMC security" means obligations or other securities which are or ever have been sold by the Federal Home Loan Mortgage Corporation pursuant to Sections 305 or 306 of the Federal Home Loan Mortgage Corporation Act (12 U.S.C. §§ 1454 and 1455).

(iii) "FNMA security" means an obligation, participation, or any instrument of or issued by, or fully guaranteed as to principal and interest by, the Federal National Mortgage Association.

(iv) "GNMA security" means an obligation, participation, or any instrument of or issued by, or fully guaranteed as to principal and interest by, the Government National Mortgage Association.

(v) "Long position" means the holding of a financial options contract with the option to make or take delivery of a financial instrument.

(vi) "Primary dealer in Government securities" means: (A) a member of the Association of Primary Dealers in United States Government Securities; or (B) any parent, subsidiary, or affiliated entity of such primary dealer where the member guarantees (to the satisfaction of the FCU's board of directors) over-the-counter sales of financial options contracts by the parent, subsidiary, or affiliated entity to a Federal credit union.

(vii) "Put" means a financial options contract which entitles the holder to sell, entirely at the holder's option, a specified quantity of a security at a specified price at any time until the stated expiration date of the contract.

(2) *Permitted Options Transactions.* A Federal credit union may, to manage risk of loss through a decrease in value of its commitments to originate real estate loans at specified interest rates, enter into long put positions on GNMA, FNMA, and FHLMC securities:

(i) if the real estate loans are to be sold on the secondary market within ninety (90) days of closing;

(ii) if the positions are entered into: (A) through a contract market designated by the Commodity Futures Trading Commission for trading such contracts, or (B) with a primary dealer in Government securities;

(iii) if the positions are entered into pursuant to written policies and procedures which are approved by the Federal credit union's board of directors, and include, at a minimum: (A) the Federal credit union's strategy in using financial options contracts and its analysis of how the strategy will reduce sensitivity to changes in price or interest rates in its commitments to originate real estate loans at specified interest rates; (B) a list of brokers or other intermediaries through which positions may be entered into; (C) quantitative limits (e.g., position and stop loss limits) on the use of financial options contracts; (D) identification of the persons involved in financial options contract transactions, including a description of these persons' qualifications, duties, and limits of authority, and description of the procedures for segregating these persons' duties, (E) a requirement for written reports for review by the Federal credit union's board of directors at its monthly meetings, or by a committee appointed by the board on a monthly basis, of: (1) the type, amount, expiration date, correlation, cost of, and current or projected income or loss from each position closed since the last board review, each position currently open and current gains or losses from such positions, and each position planned to be entered into prior to the next board review; (2) compliance with limits established on the policies and procedures; and (3) the extent to which the positions described contributed to reduction of sensitivity to changes in prices or interest rates in the Federal credit union's commitments to originate real estate loans at a specified interest rate; and

(iv) if the Federal credit union has received written permission from the appropriate NCUA Regional Director to engage in financial options contracts transactions in accordance with this § 701.21(i) and its policies and procedures as written.

(3) *Recordkeeping and Reporting.*

(i) The reports described in § 701.21 (i)(2)(iii)(E) for each month must be submitted to the appropriate NCUA Regional Office by the end of the following month. This monthly reporting requirement may be waived by the appropriate NCUA Regional Director on a case-by-case basis for those Federal credit unions with a proven record of responsible use of permitted financial options contracts.

(ii) The records described in § 701.21 (i)(2)(iii)(E) must be retained for two years from the date the financial options contracts are closed.

(4) *Accounting.* A federal credit union must account for financial options contracts transactions in accordance with generally accepted accounting principles.

a statement that its State regulatory authority agrees that it may rely on the State law parity provision as authority to convert. If a federally-insured state chartered credit union relies on a State law parity provision for authority to convert, it must indicate its State regulatory authority's position as to whether Federal law and regulations or State law will control internal governance issues in the conversion such as the requisite membership vote for conversion and the determination of a member's eligibility to vote.

(c) If it chooses, the credit union may provide the Regional Director notice of its intent to convert prior to the 90 calendar day period preceding the date of the membership vote on the conversion. In this case, the Regional Director will make a preliminary determination regarding the methods and procedures applicable to the membership vote. The Regional Director will notify the credit union within 30 calendar days of receipt of the credit union's notice of intent to convert if the Regional Director disapproves of the proposed methods and procedures applicable to the membership vote. The credit union's prior submission of the notice of intent does not relieve the credit union of its obligation to certify the results of the membership vote required by § 708a.6 or eliminate the right of the Regional Director to disapprove the actual methods and procedures applicable to the membership vote if the credit union fails to conduct the membership vote in a fair and legal manner.

§ 708a.6 Certification of vote on conversion proposal.

The board of directors of the converting credit union must certify the results of the membership vote to the Regional Director within 10 calendar days after the vote is taken. The board of directors must also certify at this time that the notice, ballot and other written materials provided to members were identical to those submitted pursuant to § 708a.5 or provide copies of any new or revised materials and an explanation of the reasons for the changes.

§ 708a.7 NCUA oversight of methods and procedures of membership vote.

(a) The Regional Director will issue a determination that the methods and procedures applicable to the membership vote are approved or disapproved within 10 calendar days of receipt from the credit union of the certification of the result of the membership vote required under § 708a.6.

(b) If the Regional Director disapproves of the methods by which the membership vote was taken or the procedures applicable to the membership vote, the Regional Director may direct that a new vote be taken.

(c) The Regional Director's review of the methods by which the membership vote was taken and the procedures applicable to the membership vote includes determining that the notice to members is accurate and not misleading, that all notices required by this section were timely, and that the membership vote was conducted in a fair and legal manner.

§ 708a.8 Other regulatory oversight of methods and procedures of membership vote.

The federal or state regulatory agency that will have jurisdiction over the financial institution after conversion must verify the membership vote and may direct that a new vote be taken, if it disapproves of the methods by which the membership vote was taken or the procedures applicable to the membership vote.

§ 708a.9 Completion of conversion.

(a) Upon receipt of approvals under § 708a.7 and § 708a.8 of this part, the credit union may complete the conversion transaction.

(b) Upon notification by the board of directors of the mutual savings bank or mutual savings association that the conversion transaction has been completed, the NCUA will cancel the insurance certificate of the credit union and, if applicable, the charter of the federal credit union.

§ 708a.10 Limit on compensation of officials.

No director or senior management official of an insured credit union may receive any economic benefit in connection with the conversion of the credit union other than compensation and other benefits paid to directors or senior management officials of the converted institution in the ordinary course of business.

§ 708a.11 Voting guidelines.

(a) A converting credit union must conduct its member vote on conversion in a fair and legal manner. These guidelines are not an exhaustive checklist that guarantees a fair and legal vote but are suggestions that provide a framework to help a credit union fulfill its regulatory obligations.

(b) While NCUA's conversion rule applies to all conversions of federally insured credit unions, federally-insured State chartered credit unions (FISCUs) are also subject to State law on conversions. NCUA's position is that a State legislature or State supervisory authority may impose conversion requirements more stringent or restrictive than NCUA's. States that permit this kind of conversion could have substantive and procedural requirements that vary from Federal law. For example, there could be different voting standards for approving a vote. While NCUA's rule requires a simple majority of those who vote to approve a conversion, some States have higher voting standards requiring two-thirds or more of those who vote. A FISCU should be careful to understand both Federal and State law to navigate the conversion process and conduct a proper vote.

(c)(1) Determining who is eligible to cast a ballot is fundamental to any vote. No conversion vote can be fair and legal if some members are improperly excluded. A converting credit union should be cautious to identify all eligible members and make certain they are included on its voting list. NCUA recommends that a converting credit union establish internal procedures to manage this task.

(2) A converting credit union should be careful to make certain its member list is accurate and complete. For example, when a credit union converts from paper record keeping to computer record keeping, some members' names may not transfer unless the credit union is careful in this regard. This same problem can arise when a credit union converts from one computer system to another where the software is not completely compatible.

(3) Problems with keeping track of who is eligible to vote can also arise when a credit union converts from a federal charter to a State charter or vice versa. NCUA is aware of an instance where a federal credit union used membership materials that allowed two or more individuals to open a joint account and also allowed each to become a member. The federal credit union later converted to a State chartered credit union that, like most other State chartered credit unions in its State, used membership materials that allowed two or more individuals to open a joint account but only allowed the first person listed on the account to become a member. The other individuals did not become members as a result of their joint account. To become members, those individuals were required to open another account where they were the first or only person listed on the account. Over time, some individuals who became members of the federal credit union as the second person listed on a joint account were treated like those individuals who were listed as the second person on a joint account opened directly with the State chartered credit union. Specifically, both of those groups were treated as non-members not entitled to vote. This example makes the point that a credit union must be diligent in maintaining a reliable membership list.

(d) NCUA's conversion rule requires a converting credit union to permit members to vote by written mail ballot or in person at a special meeting held for the purpose of voting on the conversion. Although most members may choose to vote by mail, a significant number may choose to vote in person. As a result, a converting credit union should be careful to conduct its special meeting in a manner conducive to accommodating all members that wish to attend. That includes selecting a meeting location that can accommodate the anticipated number of attendees and is conveniently located. The meeting should also be held on a day and time suitable to most members' schedules. A credit union should conduct its meeting in accordance with applicable federal and State law, its bylaws, Robert's Rules of Order or other appropriate parliamentary procedures, and determine before the meeting the nature and scope of any discussion to be permitted.

Part 717

Fair Credit Reporting

Subpart A—General Provisions

§ 717.1 Purpose.

(a) *Purpose.* The purpose of this part is to establish standards for Federal credit unions regarding consumer report information. In addition, the purpose of this part is to specify the extent to which Federal credit unions may obtain, use or share certain information. This part also contains a number of measures Federal credit unions must take to combat consumer fraud and related crimes, including identity theft.

(b) [Reserved]

§ 717.2 Examples.

The examples in this part are not exclusive. Compliance with an example, to the extent applicable, constitutes compliance with this part. Examples in a paragraph illustrate only the issue described in the paragraph and do not illustrate any other issue that may arise in this part.

§ 717.3 Definitions.

As used in this part, unless the context requires otherwise:

(a) *Act* means the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*).

(b) *Affiliate* means any company that is related by common ownership or common corporate control with another company. For example, an affiliate of a Federal credit union is a credit union service corporation (CUSO), as provided in 12 CFR part 712, that is controlled by the Federal credit union.

(c) [Reserved]

(d) *Company* means any corporation, limited liability company, business trust, general or limited partnership, association, or similar organization.

(e) *Consumer* means an individual.

(f) [Reserved]

(g) [Reserved]

(h) [Reserved]

(i) *Common ownership or common corporate control* means a relationship between two companies under which:

(1) One company has, with respect to the other company:

(i) Ownership, control, or power to vote 25 percent or more of the outstanding shares of any class of voting security of a company, directly or indirectly, or acting through one or more other persons;

(ii) Control in any manner over the election of a majority of the directors, trustees, or general partners (or individuals exercising similar functions) of a company; or

(iii) The power to exercise, directly or indirectly, a controlling influence over the management or policies of a company, as the NCUA determines; or

(iv) Example. NCUA will presume a credit union has a controlling influence over the management or policies of a CUSO, if the CUSO is 67% owned by credit unions.

(2) Any other person has, with respect to both companies, a relationship described in paragraphs (i)(1)(i)–(i)(1)(iii) of this section.

(j) [Reserved]

(k) *Medical information* means:

(1) Information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to—

(i) The past, present, or future physical, mental, or behavioral health or condition of an individual;

(ii) The provision of health care to an individual; or

(iii) The payment for the provision of health care to an individual.

(2) The term does not include:

(i) The age or gender of a consumer;

(ii) Demographic information about the consumer, including a consumer's residence address or e-mail address;

(iii) Any other information about a consumer that does not relate to the physical, mental, or behavioral health or condition of a consumer, including the existence or value of any insurance policy; or

(iv) Information that does not identify a specific consumer.

(l) *Person* means any individual, partnership, corporation, trust, estate cooperative, association, government or governmental subdivision or agency, or other entity.

(m) [Reserved]

(n) [Reserved]

(o) *You* means a Federal credit union.

Subpart D—Medical Information

§ 717.30 Obtaining or using medical information in connection with a determination of eligibility for credit.

(a) *Scope.* This section applies to:

(1) A Federal credit union that participates as a creditor in a transaction; or

(2) Any other person that participates as a creditor in a transaction involving a person described in paragraph (1).

(b) *General prohibition on obtaining or using medical information.* (1) *In general.* A creditor may not obtain or use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit, except as provided in this section.

(2) *Definitions.* (i) *Credit* has the same meaning as in section 702 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a.

(ii) *Creditor* has the same meaning as in section 702 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a.

(iii) *Eligibility, or continued eligibility, for credit* means the consumer's qualification or fitness to receive, or continue to receive, credit, including the terms on which credit is offered. The term does not include:

(A) Any determination of the consumer's qualification or fitness for employment, insurance (other than a credit insurance product), or other non-credit products or services;

(B) Authorizing, processing, or documenting a payment or transaction on behalf of the consumer in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit; or

(C) Maintaining or servicing the consumer's account in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit.

(c) *Rule of construction for obtaining and using unsolicited medical information.* (1) *In general.* A creditor does not obtain medical information in violation of the prohibition if it receives medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit without specifically requesting medical information.

(2) *Use of unsolicited medical information.* A creditor that receives unsolicited medical information in the manner described in paragraph (1) may use that information in connection with any determination of the consumer's eligibility, or continued eligibility, for credit to the extent the creditor can rely on at least one of the exceptions in § 717.30(d) or (e).

(3) *Examples.* A creditor does not obtain medical information in violation of the prohibition if, for example:

(i) In response to a general question regarding a consumer's debts or expenses, the creditor receives information that the consumer owes a debt to a hospital.

(ii) In a conversation with the creditor's loan officer, the consumer informs the creditor that the consumer has a particular medical condition.

(iii) In connection with a consumer's application for an extension of credit, the creditor requests a consumer report from a consumer reporting agency and receives medical information in the consumer report furnished by the agency even though the creditor did not specifically request medical information from the consumer reporting agency.

(d) *Financial information exception for obtaining and using medical information.*

(1) *In general.* A creditor may obtain and use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit so long as:

(i) The information is the type of information routinely used in making credit eligibility determinations, such as information relating to debts, expenses, income, benefits, assets, collateral, or the purpose of the loan, including the use of proceeds;

(ii) The creditor uses the medical information in a manner and to an extent that is no less favorable than it would use comparable information that is not medical information in a credit transaction; and

(iii) The creditor does not take the consumer's physical, mental, or behavioral health, condition or history, type of treatment, or prognosis into account as part of any such determination.

(2) *Examples.* (i) *Examples of the types of information routinely used in making credit eligibility determinations.* Paragraph (d)(1)(i) of this section permits a creditor, for example, to obtain and use information about:

(A) The dollar amount, repayment terms, repayment history, and similar information regarding medical debts to calculate, measure, or verify the repayment ability of the consumer, the use of proceeds, or the terms for granting credit;

(B) The value, condition, and lien status of a medical device that may serve as collateral to secure a loan;

(C) The dollar amount and continued eligibility for disability income or benefits related to health or a medical condition that is relied on as a source of repayment; or

(D) The identity of creditors to whom outstanding medical debts are owed in connection with an application for credit, including but not limited to, a transaction involving the consolidation of medical debts.

(ii) *Examples of uses of medical information consistent with the exception.* (A) A consumer includes on an application for credit information about two $20,000 debts. One debt is to a hospital; the other debt is to a retailer. The creditor contacts the hospital and the retailer to verify the amount and payment status of the debts. The creditor learns that both debts are more than 90 days past due. Any two debts of this size that are more than 90 days past due would disqualify the consumer under the creditor's established underwriting criteria. The creditor denies the application on the basis that the consumer has a poor repayment history on outstanding debts. The creditor has used medical information in a manner and to an extent no less favorable than it would use comparable non-medical information.

(B) A consumer indicates on an application for a $200,000 mortgage loan that she receives $15,000 in long-term disability income each year from her former employer and has no other income. Annual income of $15,000, regardless of source, would not be sufficient to support the requested amount of credit. The creditor denies the application on the basis that the projected debt-to-income ratio of the consumer does not meet the creditor's underwriting criteria. The creditor has used medical information in a manner and to an extent that is no less favorable than it would use comparable non-medical information.

(C) A consumer includes on an application for a $10,000 home equity loan that he has a $50,000 debt to a medical facility that specializes in treating a potentially terminal disease. The creditor contacts the medical facility to verify the debt and obtain the repayment history and current status of the loan. The creditor learns that the debt is current. The applicant meets the income and other requirements of the creditor's underwriting guidelines. The creditor grants the application. The creditor has used medical information in accordance with the exception.

(iii) *Examples of uses of medical information inconsistent with the exception.* (A) A consumer applies for $25,000 of credit and includes on the application information about a $50,000 debt to a hospital. The creditor contacts the hospital to verify the amount and payment status of the debt, and learns that the debt is current and that the consumer has no delinquencies in her repayment history. If the existing debt were instead owed to a retail department store, the creditor would approve the application and extend credit based on the amount and repayment history of the outstanding debt. The creditor, however, denies the application because the consumer is indebted to a hospital. The creditor has used medical information, here the identity of the medical creditor, in a manner and to an extent that is less favorable than it would use comparable non-medical information.

(B) A consumer meets with a loan officer of a creditor to apply for a mortgage loan. While filling out the loan application, the consumer informs the loan officer orally that she has a potentially terminal disease. The consumer meets the creditor's established requirements for the requested mortgage loan. The loan officer recommends to the credit committee that the consumer be denied credit because the consumer has that disease. The credit committee follows the loan officer's recommendation and denies the application because the consumer has a potentially terminal disease. The creditor has used medical information in a manner inconsistent with the exception by taking into account the consumer's physical, mental, or behavioral health, condition, or history, type of treatment, or prognosis as part of

a determination of eligibility or continued eligibility for credit.

(C) A consumer who has an apparent medical condition, such as a consumer who uses a wheelchair or an oxygen tank, meets with a loan officer to apply for a home equity loan. The consumer meets the creditor's established requirements for the requested home equity loan and the creditor typically does not require consumers to obtain a debt cancellation contract, debt suspension agreement, or credit insurance product in connection with such loans. However, based on the consumer's apparent medical condition, the loan officer recommends to the credit committee that credit be extended to the consumer only if the consumer obtains a debt cancellation contract, debt suspension agreement, or credit insurance product. The credit committee agrees with the loan officer's recommendation. The loan officer informs the consumer that the consumer must obtain a debt cancellation contract, debt suspension agreement, or credit insurance product to qualify for the loan. The consumer obtains one of these products from a third party and the creditor approves the loan. The creditor has used medical information in a manner inconsistent with the exception by taking into account the consumer's physical, mental, or behavioral health, condition, or history, type of treatment, or prognosis in setting conditions on the consumer's eligibility for credit.

(e) *Specific exceptions for obtaining and using medical information.* (1) *In general.* A creditor may obtain and use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit—

(i) To determine whether the use of a power of attorney or legal representative that is triggered by a medical event or condition is necessary and appropriate or whether the consumer has the legal capacity to contract when a person seeks to exercise a power of attorney or act as legal representative for a consumer based on an asserted medical event or condition;

(ii) To comply with applicable requirements of local, State, or Federal laws;

(iii) To determine, at the consumer's request, whether the consumer qualifies for a legally permissible special credit program or credit-related assistance program that is—

(A) Designed to meet the special needs of consumers with medical conditions; and

(B) Established and administered pursuant to a written plan that—

(*1*) Identifies the class of persons that the program is designed to benefit; and

(*2*) Sets forth the procedures and standards for extending credit or providing other credit-related assistance under the program.

(iv) To the extent necessary for purposes of fraud prevention or detection;

(v) In the case of credit for the purpose of financing medical products or services, to determine and verify the medical purpose of a loan and the use of proceeds;

(vi) Consistent with safe and sound practices, if the consumer or the consumer's legal representative specifically requests that the creditor use medical information in determining the consumer's eligibility, or continued eligibility, for credit, to accommodate the consumer's particular circumstances, and such request is documented by the creditor;

(vii) Consistent with safe and sound practices, to determine whether the provisions of a forbearance practice or program that is triggered by a medical event or condition apply to a consumer;

(viii) To determine the consumer's eligibility for, the triggering of, or the reactivation of a debt cancellation contract or debt suspension agreement if a medical condition or event is a triggering event for the provision of benefits under the contract or agreement; or

(ix) To determine the consumer's eligibility for, the triggering of, or the reactivation of a credit insurance product if a medical condition or event is a triggering event for the provision of benefits under the product.

(2) *Example of determining eligibility for a special credit program or credit assistance program.* A not-for-profit organization establishes a credit assistance program pursuant to a written plan that is designed to assist disabled veterans in purchasing homes by subsidizing the down payment for the home purchase mortgage loans of qualifying veterans. The organization works through mortgage lenders and requires mortgage lenders to obtain medical information about the disability of any consumer that seeks to qualify for the program, use that information to verify the consumer's eligibility for the program, and forward that information to the organization. A consumer who is a veteran applies to a creditor for a home purchase mortgage loan. The creditor informs the consumer

about the credit assistance program for disabled veterans and the consumer seeks to qualify for the program. Assuming that the program complies with all applicable law, including applicable fair lending laws, the creditor may obtain and use medical information about the medical condition and disability, if any, of the consumer to determine whether the consumer qualifies for the credit assistance program.

(3) *Examples of verifying the medical purpose of the loan or the use of proceeds.* (i) If a consumer applies for $10,000 of credit for the purpose of financing vision correction surgery, the creditor may verify with the surgeon that the procedure will be performed. If the surgeon reports that surgery will not be performed on the consumer, the creditor may use that medical information to deny the consumer's application for credit, because the loan would not be used for the stated purpose.

(ii) If a consumer applies for $10,000 of credit for the purpose of financing cosmetic surgery, the creditor may confirm the cost of the procedure with the surgeon. If the surgeon reports that the cost of the procedure is $5,000, the creditor may use that medical information to offer the consumer only $5,000 of credit.

(iii) A creditor has an established medical loan program for financing particular elective surgical procedures. The creditor receives a loan application from a consumer requesting $10,000 of credit under the established loan program for an elective surgical procedure. The consumer indicates on the application that the purpose of the loan is to finance an elective surgical procedure not eligible for funding under the guidelines of the established loan program. The creditor may deny the consumer's application because the purpose of the loan is not for a particular procedure funded by the established loan program.

(4) *Examples of obtaining and using medical information at the request of the consumer.* (i) If a consumer applies for a loan and specifically requests that the creditor consider the consumer's medical disability at the relevant time as an explanation for adverse payment history information in his credit report, the creditor may consider such medical information in evaluating the consumer's willingness and ability to repay the requested loan to accommodate the consumer's particular circumstances, consistent with safe and sound practices. The creditor may also decline to consider such medical information to accommodate the consumer, but may evaluate the consumer's application in accordance with its otherwise applicable underwriting criteria. The creditor may not deny the consumer's application or otherwise treat the consumer less favorably because the consumer specifically requested a medical accommodation, if the creditor would have extended the credit or treated the consumer more favorably under the creditor's otherwise applicable underwriting criteria.

(ii) If a consumer applies for a loan by telephone and explains that his income has been and will continue to be interrupted on account of a medical condition and that he expects to repay the loan by liquidating assets, the creditor may, but is not required to, evaluate the application using the sale of assets as the primary source of repayment, consistent with safe and sound practices, provided that the creditor documents the consumer's request by recording the oral conversation or making a notation of the request in the consumer's file.

(iii) If a consumer applies for a loan and the application form provides a space where the consumer may provide any other information or special circumstances, whether medical or nonmedical, that the consumer would like the creditor to consider in evaluating the consumer's application, the creditor may use medical information provided by the consumer in that space on that application to accommodate the consumer's application for credit, consistent with safe and sound practices, or may disregard that information.

(iv) If a consumer specifically requests that the creditor use medical information in determining the consumer's eligibility, or continued eligibility, for credit and provides the creditor with medical information for that purpose, and the creditor determines that it needs additional information regarding the consumer's circumstances, the creditor may request, obtain, and use additional medical information about the consumer as necessary to verify the information provided by the consumer or to determine whether to make an accommodation for the consumer. The consumer may decline to provide additional information, withdraw the request for an accommodation, and have the application considered under the creditor's otherwise applicable underwriting criteria.

(v) If a consumer completes and signs a credit application that is not for medical purpose credit and the application contains boilerplate language that routinely requests

medical information from the consumer or that indicates that by applying for credit the consumer authorizes or consents to the creditor obtaining and using medical information in connection with a determination of the consumer's eligibility, or continued eligibility, for credit, the consumer has not specifically requested that the creditor obtain and use medical information to accommodate the consumer's particular circumstances.

(5) *Example of a forbearance practice or program.* After an appropriate safety and soundness review, a creditor institutes a program that allows consumers who are or will be hospitalized to defer payments as needed for up to three months, without penalty, if the credit account has been open for more than one year and has not previously been in default, and the consumer provides confirming documentation at an appropriate time. A consumer is hospitalized and does not pay her bill for a particular month. This consumer has had a credit account with the creditor for more than one year and has not previously been in default. The creditor attempts to contact the consumer and speaks with the consumer's adult child, who is not the consumer's legal representative. The adult child informs the creditor that the consumer is hospitalized and is unable to pay the bill at that time. The creditor defers payments for up to three months, without penalty, for the hospitalized consumer and sends the consumer a letter confirming this practice and the date on which the next payment will be due.

§ 717.31 Limits on redisclosure of information.

(a) *Scope*. This section applies to Federal credit unions.

(b) *Limits on redisclosure.* If a Federal credit union receives medical information about a consumer from a consumer reporting agency or its affiliate, the person must not disclose that information to any other person, except as necessary to carry out the purpose for which the information was initially disclosed, or as otherwise permitted by statute, regulation, or order.

§ 717.32 Sharing medical information with affiliates.

(a) *Scope.* This section applies to Federal credit unions.

(b) *In general.* The exclusions from the term "consumer report" in section 603(d)(2) of the Act that allow the sharing of information with affiliates do not apply if a Federal credit union communicates to an affiliate—

(1) Medical information;

(2) An individualized list or description based on the payment transactions of the consumer for medical products or services; or

(3) An aggregate list of identified consumers based on payment transactions for medical products or services.

(c) *Exceptions.* A Federal credit union may rely on the exclusions from the term "consumer report" in section 603(d)(2) of the Act to communicate the information in paragraph (b) to an affiliate—

(1) In connection with the business of insurance or annuities (including the activities described in section 18B of the model Privacy of Consumer Financial and Health Information Regulation issued by the National Association of Insurance Commissioners, as in effect on January 1, 2003);

(2) For any purpose permitted without authorization under the regulations promulgated by the Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA);

(3) For any purpose referred to in section 1179 of HIPAA;

(4) For any purpose described in section 502(e) of the Gramm-Leach-Bliley Act;

(5) In connection with a determination of the consumer's eligibility, or continued eligibility, for credit consistent with § 717.30; or

(6) As otherwise permitted by order of the NCUA.

Subpart I—Duties of Users of Consumer Reports Regarding Identity Theft

§ 717.80–717.82 [Reserved]

§ 717.83 Disposal of consumer information.

(a) *In general.* You must properly dispose of any consumer information that you maintain or otherwise possess in a manner consistent with the Guidelines for Safeguarding Member Information, in appendix A to part 748 of this chapter.

(b) *Examples.* Appropriate measures to properly dispose of consumer information include the fol-

lowing examples. These examples are illustrative only and are not exclusive or exhaustive methods for complying with this section.

(1) Burning, pulverizing, or shredding papers containing consumer information so that the information cannot practicably be read or reconstructed.

(2) Destroying or erasing electronic media containing consumer information so that the information cannot practicably be read or reconstructed.

(c) *Rule of construction.* This section does not:

(1) Require you to maintain or destroy any record pertaining to a consumer that is not imposed under any other law; or

(2) Alter or affect any requirement imposed under any other provision of law to maintain or destroy such a record.

(d) *Definitions.* As used in this section:

(1) *Consumer information* means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report and that is maintained or otherwise possessed by or on behalf of the credit union for a business purpose. Consumer information also means a compilation of such records. The term does not include any record that does not identify an individual.

(i) *Consumer information* includes:

(A) A consumer report that you obtain;

(B) Information from a consumer report that you obtain from your affiliate after the consumer has been given a notice and has elected not to opt out of that sharing;

(C) Information from a consumer report that you obtain about an individual who applies for but does not receive a loan, including any loan sought by an individual for a business purpose;

(D) Information from a consumer report that you obtain about an individual who guarantees a loan (including a loan to a business entity); or

(E) Information from a consumer report that you obtain about an employee or prospective employee.

(ii) *Consumer information* does not include:

(A) Aggregate information, such as the mean credit score, derived from a group of consumer reports; or

(B) Blind data, such as payment history on accounts that are not personally identifiable, you use for developing credit scoring models or for other purposes.

(2) *Consumer report* has the same meaning as set forth in the Fair Credit Reporting Act, 15 U.S.C. 1681a(d). The meaning of consumer report is broad and subject to various definitions, conditions and exceptions in the Fair Credit Reporting Act. It includes written or oral communications from a consumer reporting agency to a third party of information used or collected for use in establishing eligibility for credit or insurance used primarily for personal, family or household purposes, and eligibility for employment purposes. Examples include credit reports, bad check lists, and tenant screening reports.

Part 748

Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance

§ 748.0 Security program.

(a) Each federally-insured credit union will develop a written security program within 90 days of the effective date of insurance.

(b) The security program will be designed to:

(1) Protect each credit union office from robberies, burglaries, larcenies, and embezzlement;

(2) Ensure the security and confidentiality of member records, protect against the anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to a member;

(3) Respond to incidents of unauthorized access to or use of member information that could result in substantial harm or serious inconvenience to a member;

(4) Assist in the identification of persons who commit or attempt such actions and crimes, and

(5) Prevent destruction of vital records, as defined in 12 CFR part 749.

(c) Each Federal credit union, as part of its information security program, must properly dispose of any consumer information the Federal credit union maintains or otherwise possesses, as required under § 717.83 of this chapter.

§ 748.1 Filing of reports.

(a) *Compliance Report.* Each federally-insured credit union shall file with the regional director an annual statement certifying its compliance with the requirements of this Part. The statement shall be dated and signed by the president or other managing officer of the credit union. The statement is contained on the Report of Officials which is submitted annually by federally-insured credit unions after the election of officials. In the case of federally-insured state-chartered credit unions, this statement can be mailed to the regional director via the state supervisory authority, if desired. In any event, a copy of the statement shall always be sent to the appropriate state supervisory authority.

(b) *Catastrophic Act Report.* Each federally-insured credit union will notify the regional director within 5 business days of any catastrophic act that occurs at its office(s). A catastrophic act is any natural disaster such as a flood, tornado, earthquake, etc., or major fire or other disaster resulting in some physical destruction or damage to the credit union. Within a reasonable time after a catastrophic act occurs, the credit union shall ensure that a record of the incident is prepared and filed at its main office. In the preparation of such record, the credit union should include information sufficient to indicate the office where the catastrophic act occurred; when it took place; the amount of the loss, if any; whether any operational or mechanical deficiency(ies) might have contributed to the catastrophic act; and what has been done or is planned to be done to correct the deficiency(ies).

(c) *Suspicious Activity Report.* (1) Each federally-insured credit union will report any crime or suspected crime that occurs at its office(s), utilizing NCUA Form 2362, Suspicious Activity Report (SAR), within thirty calendar days after discovery. Each federally-insured credit union must follow the instructions and reporting requirements accompanying the SAR. Copies of the SAR may be obtained from the appropriate NCUA Regional Office.

(2) Each federally-insured credit union shall maintain a copy of any SAR that it files and the original of all attachments to the report for a period of five years from the date of the report, unless the credit union is informed in writing by the National Credit Union Administration that the materials may be discarded sooner.

(3) Failure to file a SAR in accordance with the instructions accompanying the report may subject the federally-insured credit union, its officers, directors, agents or other institution-affiliated parties to the assessment of civil money penalties or other administrative actions.

(4) Filing of Suspicious Activity Reports will ensure that law enforcement agencies and NCUA are promptly notified of actual or suspected crimes. Information contained on SARs will be entered into an interagency database and will assist the federal government in taking appropriate action.

§ 748.2 Procedures for monitoring Bank Secrecy Act (BSA) compliance.

(a) *Purpose.* This Section is issued to ensure that all federally-insured credit unions establish and maintain procedures reasonably designed to assure and monitor compliance with the requirements of Subchapter II of Chapter 53 of Title 31, United States Code, the Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act, and the implementing regulations promulgated thereunder by the Department of Treasury, 31 C.F.R. Part 103.

(b) *Establishment of a BSA compliance program.* (1) *Program requirement.* Each federally-insured credit union shall develop and provide for the continued administration of a program reasonably designed to assure and monitor compliance with the recordkeeping and recording requirements set forth in subchapter II of chapter 53 of title 31, United States Code and the implementing regulations issued by the Department of the Treasury at 31 CFR part 103. The compliance program must be written, approved by the credit union's board of directors, and reflected in the minutes of the credit union.

(2) *Customer identification program.* Each federally-insured credit union is subject to the requirements of 31 U.S.C. 5318(l) and the implementing regulation jointly promulgated by the NCUA and the Department of the Treasury at 31 CFR 103.121, which require a customer identification program to be implemented as part of the BSA compliance program required under this section.

(c) *Contents of Compliance Program.* Such compliance program shall at a minimum—

(1) Provide for a system of internal controls to assure ongoing compliance;

(2) Provide for independent testing for compliance to be conducted by credit union personnel or outside parties;

(3) Designate an individual responsible for coordinating and monitoring day-to-day compliance; and

(4) Provide training for appropriate personnel.

tions as required by paragraph D.2. As part of this monitoring, a credit union should review audits, summaries of test results, or other equivalent evaluations of its service providers.

E. *Adjust the Program.* Each credit union should monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its member information, internal or external threats to information, and the credit union's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to member information systems.

F. *Report to the Board.* Each credit union should report to its board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the credit union's compliance with these guidelines. The report should discuss material matters related to its program, addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for changes in the information security program.

G. *Implement the Standards.*

1. *Effective date.* Each credit union must implement an information security program pursuant to the objectives of these Guidelines by July 1, 2001.

2. *Two-year grandfathering of agreements with service providers.* Until July 1, 2003, a contract that a credit union has entered into with a service provider to perform services for it or functions on its behalf satisfies the provisions of paragraph III.D., even if the contract does not include a requirement that the servicer maintain the security and confidentiality of member information, as long as the credit union entered into the contract on or before March 1, 2001.

3. *Effective date for measures relating to the disposal of consumer information.* Each Federal credit union must properly dispose of consumer information in a manner consistent with these Guidelines by July 1, 2005.

4. *Exception for existing agreements with service providers relating to the disposal of consumer information.* Notwithstanding the requirement in paragraph III.G.3., a Federal credit union's existing contracts with its service providers with regard to any service involving the disposal of consumer information should implement the objectives of these Guidelines by July 1, 2006.

Appendix B to Part 748—Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice

I. Background

This Guidance in the form of Appendix B to NCUA's Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance regulation,[29] interprets section 501(b) of the Gramm-Leach-Bliley Act ("GLBA") and describes response programs, including member notification procedures, that a federally insured credit union should develop and implement to address unauthorized access to or use of member information that could result in substantial harm or inconvenience to a member. The scope of, and definitions of terms used in, this Guidance are identical to those of Appendix A to Part 748 (Appendix A). For example, the term "member information" is the same term used in Appendix A, and means any record containing nonpublic personal information about a member, whether in paper, electronic, or other form, maintained by or on behalf of the credit union.

A. Security Guidelines

Section 501(b) of the GLBA required the NCUA to establish appropriate standards for credit unions subject to its jurisdiction that include administrative, technical, and physical safeguards to protect the security and confidentiality of member information. Accordingly, the NCUA amended Part 748 of its rules to require credit unions to develop appropriate security programs, and issued Appendix A, reflecting its expectation that every federally insured credit union would develop an information security program designed to:

1. Ensure the security and confidentiality of member information;

2. Protect against any anticipated threats or hazards to the security or integrity of such information; and

3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any member.

B. Risk Assessment and Controls

1. Appendix A directs every credit union to assess the following risks, among others, when developing its information security program:

a. Reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of member information or member information systems;

b. The likelihood and potential damage of threats, taking into consideration the sensitivity of member information; and

c. The sufficiency of policies, procedures, member information systems, and other arrangements in place to control risks.[30]

2. Following the assessment of these risks, Appendix A directs a credit union to design a program to address the identified risks. The particular security measures a credit union should adopt will depend upon the risks presented by the complexity and scope of its business. At a minimum, the credit union should consider the specific security measures enumerated in Appendix A,[31] and adopt those that are appropriate for the credit union, including:

a. Access controls on member information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing member information to unauthorized individuals who may seek to obtain this information through fraudulent means;

b. Background checks for employees with responsibilities for access to member information; and

c. Response programs that specify actions to be taken when the credit union suspects or detects that unauthorized individuals have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies.[32]

C. Service Providers

Appendix A advises every credit union to require its service providers by contract to implement appropriate measures designed to protect against unauthorized access to or use of member information that could result in substantial harm or inconvenience to any member.[33]

[29] 12 CFR Part 748.

[30] *See* 12 CFR Part 748, Appendix A, Paragraph III.B.

[31] *See* Appendix A, paragraph III.C.

[32] *See* Appendix A, Paragraph III.C.

[33] *See* Appendix A, Paragraph III.B. and III.D. Further, the NCUA notes that, in addition to contractual obligations

II. Response Program

i. Millions of Americans, throughout the country, have been victims of identity theft.[34] Identity thieves misuse personal information they obtain from a number of sources, including credit unions, to perpetrate identity theft. Therefore, credit unions should take preventative measures to safeguard member information against such attempts to gain unauthorized access to the information. For example, credit unions should place access controls on member information systems and conduct background checks for employees who are authorized to access member information.[35] However, every credit union should also develop and implement a risk-based response program to address incidents of unauthorized access to member information in member information systems that occur nonetheless.[36] A response program should be a key part of a credit union's information security program.[37] The program should be appropriate to the size and complexity of the credit union and the nature and scope of its activities.

ii. In addition, each credit union should be able to address incidents of unauthorized access to member information in member information systems maintained by its domestic and foreign service providers. Therefore, consistent with the obligations in this Guidance that relate to these arrangements, and with existing guidance on this topic issued by the NCUA,[38] a credit union's contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to or use of the credit union's member information, including notification of the credit union as soon as possible of any such incident, to enable the institution to expeditiously implement its response program.

A. Components of a Response Program

1. At a minimum, a credit union's response program should contain procedures for the following:

a. Assessing the nature and scope of an incident, and identifying what member information systems and types of member information have been accessed or misused;

b. Notifying the appropriate NCUA Regional Director, and, in the case of state-chartered credit unions, its applicable state supervisory authority, as soon as possible when the credit union becomes aware of an incident involving unauthorized access to or use of sensitive member information as defined below.

c. Consistent with the NCUA's Suspicious Activity Report ("SAR") regulations,[39] notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;

d. Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of member information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; [40] and

e. Notifying members when warranted.

2. Where an incident of unauthorized access to member information involves member infor-

---

to a credit union, a service provider may be required to implement its own comprehensive information security program in accordance with the Safeguards Rule promulgated by the Federal Trade Commission ("FTC"), 12 CFR Part 314.

[34] The FTC estimates that nearly 10 million Americans discovered they were victims of some form of identify theft in 2002. *See* The Federal Trade Commission, *Identity Theft Survey Report,* (September 2003), available at *http://www.ftc.gov/os/2003/09synovatereport.pdf.*

[35] Credit unions should also conduct background checks of employees to ensure that the credit union does not violate 12 U.S.C. 1785(d), which prohibits a credit union from hiring an individual convicted of certain criminal offenses or who is subject to a prohibition order under 12 U.S.C. 1786(g).

[36] Under 12 CFR Part 748, Appendix A, a credit union's *member information systems* consists of all of the methods used to access, collect, store, use, transmit, protect, or dispose of member information, including the systems maintained by its service providers. *See* 12 CFR Part 748, Appendix A, Paragraph I.C.2.d.

[37] *See* FFIEC Information Technology Examination Handbook, Information Security Booklet, (December, 2002), available at *http://www.ffiec.gov/ffiecinfobase/html—pages/it—01.htm1#infosec,* for additional guidance on preventing, detecting, and responding to intrusions into financial institution computer systems.

[38] *See* FFIEC Information Technology Examination Handbook, Outsourcing Technology Services Booklet, (June 2004), available at *http://www.ffiec.gov/ffiecinfobase/html—pages/it—01.htm1#outscouring* for additional guidance on managing outsourced relationships.

[39] A credit union's obligation to file a SAR is set out in the NCUA's SAR regulations and guidance. *See* 12 CFR Part 748.1(c); NCUA Letter to Credit Unions No. 04–CU–03, Suspiciouis Activity Reports, March 2004; NCUA Regulatory Alert No. 04–RA–01, The Suspicious Activity Report (SAR) Activity Review—Trends, Tips, & Isues, Issue 6, November 2003, February 2004.

[40] *See* FFIEC Information Technology Examination Handbook, Information Security Booklet, (December 2002), pp. 68–74.

mation systems maintained by a credit union's service providers, it is the responsibility of the credit union to notify the credit union's members and regulator. However, a credit union may authorize or contract with its service provider to notify the credit union's members or regulators on its behalf.

III. Member Notice

i. Credit unions have an affirmative duty to protect their members' information against unauthorized access or use. Notifying members of a security incident involving the unauthorized access or use of the member's information in accordance with the standard set forth below is a key part of that duty.

ii. Timely notification of members is important to manage a credit union's reputation risk. Effective notice also may reduce a credit union's legal risk, assist in maintaining good member relations, and enable the credit union's members to take steps to protect themselves against the consequences of identity theft. When member notification is warranted, a credit union may not forgo notifying its customers of an incident because the credit union believes that it may be potentially embarrassed or inconvenienced by doing so.

A. Standard for Providing Notice

When a credit union becomes aware of an incident of unauthorized access to sensitive member information, the credit union should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the credit union determines that misuse of its information about a member has occurred or is reasonably possible, it should notify the affected member as soon as possible. Member notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the credit union with a written request for the delay. However, the credit union should notify its members as soon as notification will no longer interfere with the investigation.

1. Sensitive Member Information

Under Part 748.0, a credit union must protect against unauthorized access to or use of member information that could result in substantial harm or inconvenience to any member. Substantial harm or inconvenience is most likely to result from improper access to *sensitive member information* because this type of information is most likely to be misused, as in the commission of identity theft.

For purposes of this Guidance, sensitive member information means a member's name, address, or telephone number, in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the member's account. *Sensitive member information* also includes any combination of components of member information that would allow someone to log onto or access the member's account, such as user name and password or password and account number.

2. Affected Members

If a credit union, based upon its investigation, can determine from its logs or other data precisely which members' information has been improperly accessed, it may limit notification to those members with regard to whom the credit union determines that misuse of their information has occurred or is reasonably possible. However, there may be situations where the credit union determines that a group of files has been accessed improperly, but is unable to identify which specific member's information has been accessed. If the circumstances of the unauthorized access lead the credit union to determine that misuse of the information is reasonably possible, it should notify all members in the group.

B. Content of Member Notice

1. Member notice should be given in a clear and conspicuous manner. The notice should describe the incident in general terms and the type of member information that was the subject of unauthorized access or use. It also should generally describe what the credit union has done to protect the members' information from further unauthorized access. In addition, it should include a telephone number that members can call for further information and assistance.[41] The notice also should remind members of the need to remain vigilant over the next twelve to twenty-four months, and to promptly

[41] The credit union should, therefore, ensure that it has reasonable policies and procedures in place, including trained personnel, to respond appropriately to member inquiries and requests for assistance.

report incidents of suspected identity theft to the credit union. The notice should include the following additional items, when appropriate:

a. A recommendation that the member review account statements and immediately report any suspicious activity to the credit union;

b. A description of fraud alerts and an explanation of how the member may place a fraud alert in the member's consumer reports to put the member's creditors on notice that the member may be a victim of fraud;

c. A recommendation that the member periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;

d. An explanation of how the member may obtain a credit report free of charge; and

e. Information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft. The notice should encourage the member to report any incidents of identity theft to the FTC, and should provide the FTC's Web site address and toll-free telephone number that members may use to obtain the identity theft guidance and report suspected incidents of identity theft.[42]

2. NCUA encourages credit unions to notify the nationwide consumer reporting agencies prior to sending notices to a large number of members that include contact information for the reporting agencies.

C. Delivery of Member Notice

Member notice should be delivered in any manner designed to ensure that a member can reasonably be expected to receive it. For example, the credit union may choose to contact all members affected by telephone or by mail, or by electronic mail for those members for whom it has a valid e-mail address and who have agreed to receive communications electronically.

---

[42] Currently, the FTC Web site for the ID Theft brochure and the FTC Hotline phone number are *http://www.ftc.gov/idtheft* and 1–877–IDTHEFT. The credit union may also refer members to any materials developed pursuant to section 15(1)(b) of the FACT Act (educational materials developed by the FTC to teach the public how to prevent identity theft).

when NCUA notifies you that the request cannot be processed in the specified time limit.

§ 792.16 What unusual circumstances can delay NCUA's response?

(a) In unusual circumstances, the time limits for responding to your request (or your appeal) may be extended by NCUA. If NCUA extends the time it will provide you with written notice, setting forth the reasons for such extension and the date on which a determination is expected to be dispatched. Our notice will not specify a date that would result in an extension for more than 10 working days, except as set forth in paragraph (c) of this section. The unusual circumstances that can delay NCUA's response to your request are:

(1) The need to search for, and collect the requested records from field facilities or other establishments that are separate from the office processing the request;

(2) The need to search for, collect, and appropriately examine a voluminous amount of separate and distinct records which are demanded in a single request; or

(3) The need for consultation, which will be conducted with all practicable speed, with another agency having substantial interest in the determination of the request or among two or more components of NCUA having a substantial interest in the subject matter.

(b) If you, or you and a group of others acting in concert, submit multiple requests that NCUA believes actually constitute a single request, which would otherwise satisfy the unusual circumstances criteria specified in this section, and the requests involve related matters, then NCUA may aggregate those requests and the provisions of § 792.15(b) will apply.

(c) If NCUA sends you an extension notice, it will also advise you that you can either limit the scope of your request so that it can be processed within the statutory time limit or agree to an alternative time frame for processing your request.

§ 792.17 What can I do if the time limit passes and I still have not received a response?

You can file suit against NCUA because you will be deemed to have exhausted your administrative remedies if NCUA fails to comply with the time limit provisions of this subpart. If NCUA can show that exceptional circumstances exist and that it is exercising due diligence in responding to your request, the court may retain jurisdiction and allow NCUA to complete its review of the records. In determining whether exceptional circumstances exist, the court may consider your refusal to modify the scope of your request or arrange an alternative time frame for processing after being given the opportunity to do so by NCUA, when it notifies you of the existence of unusual circumstances as set forth in § 792.16.

Expedited Processing

§ 792.18 What if my request is urgent and I cannot wait for the records?

You may request expedited processing of your request if you can show a compelling need for the records. In cases where your request for expedited processing is granted or if NCUA has determined to expedite the response, it will be processed as soon as practicable.

(a) To demonstrate a compelling need for expedited processing, you must provide a certified statement. The statement, certified by you to be true and correct to the best of your knowledge and belief, must demonstrate that:

(1) The failure to obtain the records on an expedited basis could reasonably be expected to pose an imminent threat to the life or physical safety of an individual; or

(2) The requester is a representative of the news media, as defined in § 792.20, and there is urgency to inform the public concerning actual or alleged NCUA activity.

(b) In response to a request for expedited processing, the Information Center will notify you of the determination within ten days of receipt of the request. If the Information Center denies your request for expedited processing, you may file an appeal pursuant to the procedures set forth in § 792.28, and NCUA will expeditiously respond to the appeal.

(c) The Information Center will normally process requests in the order they are received in the separate processing tracks. However, in NCUA's discretion, a particular request may be processed out of turn.

Fees

§ 792.19 How does NCUA calculate the fees for processing my request?

We will charge you our allowable direct costs, unless they are less than the cost of billing you. Direct costs means those expenditures that NCUA actually incurs in searching for, duplicating and reviewing documents to respond to a FOIA request. Search means all time spent looking for material that is responsive to a request, including page-by-page or line-by-line identification of material within documents. Searches may be done manually or by computer. Search does not include modification of an existing program or system that would significantly interfere with the operation of an automated information system. Review means examining documents to determine whether any portion should be withheld and preparing documents for disclosure. Fees are subject to change as costs increase. The current rate schedule is available on our web site at http://www.ncua.gov. We may contract with the private sector to locate, reproduce or disseminate records. NCUA will not contract out responsibilities that FOIA requires it to discharge, such as determining the applicability of an exemption, or determining whether to waive or reduce fees. The following labor and duplication rate calculations apply:

(a) NCUA will charge fees at the following rates for manual searches for and review of records:

(1) If search/review is done by clerical staff, the hourly rate for CU–5, plus 16% of that rate to cover benefits;

(2) If search/review is done by professional staff, the hourly rate for CU–13, plus 16% of that rate to cover benefits.

(b) NCUA will charge fees at the hourly rate for CU–13, plus 16% of that rate to cover benefits, plus the hourly cost of operating the computer for computer searches for records.

(c) NCUA will charge the following duplication fees:

(1) The per-page fee for paper copy reproduction of a document is $.05;

(2) The fee for documents generated by computer is the hourly fee for the computer operator, plus the cost of materials (computer paper, tapes, labels, etc.);

(3) If any other method of duplication is used, NCUA will charge the actual direct cost of duplication.

§ 792.20 What are the charges for each fee category?

The fee category definitions are:

(a) *Commercial use request* means a request from or on behalf of one who seeks information for a use or purpose that furthers the commercial, trade, or profit interests of the requester or the person on whose behalf the request is made.

(b) *Educational institution* means a preschool, an elementary or secondary school, an institution of undergraduate higher education, an institution of graduate higher education, an institution of professional education, and an institution of vocational education operating a program or programs of scholarly research.

(c) *Noncommercial scientific institution* means an institution that is not operated for a "commercial" purpose as that term is used in paragraph (a) of this section and is operated solely for the purpose of conducting scientific research, the results of which are not intended to promote any particular product or industry.

(d) *Representative of the news media* means any person actively gathering news for an entity that is organized and operated to publish or broadcast news to the public. Included within the meaning of public is the credit union community. The term news means information that is about current events or that would be of current interest to the public.

You may consult the following chart to find the fees applicable to your request:

If your fee category is	You'll receive	And you'll be charged
Commercial use	0 hours free search 0 hours free review 0 free pages	search time review time duplication
Educational institution, noncommercial scientific institution, newsmedia.	Unlimited free search hours Unlimited free review hours 100 free pages	duplication
All others	2 hours free search Unlimited free review hours.	search time

If your fee category is	You'll receive	And you'll be charged
	100 free pages	duplication

§ 792.21 Will NCUA provide a fee estimate?

NCUA will notify you of the estimated amount if fees are likely to exceed $25, unless you have indicated in advance a willingness to pay fees as high as those anticipated. You will then have the opportunity to confer with NCUA personnel to reformulate the request to meet your needs at a lower cost.

§ 792.22 What will NCUA charge for other services?

Complying with requests for special services is entirely at the discretion of NCUA. NCUA will recover the full costs of providing such services to the extent it elects to provide them.

§ 792.23 Can I avoid charges by sending multiple, small requests?

You may not file multiple requests, each seeking portions of a document or similar documents, solely to avoid payment of fees. If this is done, NCUA may aggregate any such requests and charge you accordingly.

§ 792.24 Can NCUA charge me interest if I fail to pay my bill?

NCUA can assess interest charges on an unpaid bill starting on the 31st day following the date of the bill. If you fail to pay your bill within 30 days, interest will be at the rate prescribed in 31 U.S.C. 3717, and will accrue from the date of the billing.

§ 792.25 Will NCUA charge me if the records are not found or are determined to be exempt?

NCUA may assess fees for time spent searching and reviewing, even if it fails to locate the records or if records located are determined to be exempt from disclosure.

§ 792.26 Will I be asked to pay fees in advance?

NCUA will require you to give an assurance of payment or an advance payment only when:

(a) NCUA estimates or determines that allowable charges that you may be required to pay are likely to exceed $250. NCUA will notify you of the likely cost and obtain satisfactory assurance of full payment where you have a history of prompt payment of FOIA fees, or require an advance payment of an amount up to the full estimated charges in the case where you have no history of payment; or

(b) You have previously failed to pay a fee charged in a timely fashion. NCUA may require you to pay the full amount owed, plus any applicable interest, or demonstrate that you have, in fact, paid the fee, and to make an advance payment of the full amount of the estimated fee before we begin to process a new request or a pending request from you.

(c) If you are required to make an advance payment of fees, then the administrative time limits prescribed in § 792.16 will begin only after NCUA has received the fee payments described.

Fee Waiver or Reduction

§ 792.27 Can fees be reduced or waived?

You may request that NCUA waive or reduce fees if disclosure of the information you request is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government, and is not primarily in your commercial interest.

(a) NCUA will make a determination of whether the public interest requirement above is met based on the following factors:

(1) Whether the subject of the requested records concerns the operations or activities of the government;

(2) Whether the disclosure is likely to contribute to an understanding of government operations or activities;

(3) Whether disclosure of the requested information will contribute to public understanding; and

(4) Whether the disclosure is likely to contribute significantly to public understanding of government operations or activities,

(b) If the public interest requirement is met, NCUA will make a determination on the commer-

cial interest requirement based upon the following factors:

(1) Whether you have a commercial interest that would be furthered by the requested disclosure; and if so

(2) Whether the magnitude of your commercial interest is sufficiently large in comparison with the public interest in disclosure, that disclosure is primarily in your commercial interest.

(c) If the required public interest exists and your commercial interest is not primary in comparison, NCUA will waive or reduce fees.

(d) If you are not satisfied with our determination on your fee waiver or reduction request, you may submit an appeal to the General Counsel in accordance with § 792.28.

Appeals

§ 792.28 What if I am not satisfied with the response I receive?

If you are not satisfied with NCUA's response to your request, you can file an administrative appeal. Your appeal must be in writing and must be filed within 30 days from receipt of the initial determination (in cases of denials of an entire request, or denial of a request for fee waiver or reduction), or from receipt of any records being made available pursuant to the initial determination (in cases of partial denials.) In its response to your initial request, the Freedom of Information Act Officer or the Inspector General (or designee), will notify you that you may appeal any adverse determination to the Office of General Counsel. The General Counsel, or designee, as set forth in this paragraph, will:

(a) Make a determination with respect to any appeal within 20 days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of such appeal. If, on appeal, the denial of the request for records is, in whole or in part, upheld, the Office of General Counsel will notify you of the provisions for judicial review of that determination under FOIA. Where you do not address your request or appeal to the proper official, the time limitations stated above will be computed from the receipt of the request or appeal by the proper official.

(b) The General Counsel is the official responsible for determining all appeals from initial determinations. In case of this person's absence, the appropriate officer acting in the General Counsel's stead will make the appellate determination, unless such officer was responsible for the initial determination, in which case the Vice-Chairman of the NCUA Board will make the appellate determination.

(c) All appeals should be addressed to the General Counsel in the Central Office and should be clearly identified as such on the envelope and in the letter of appeal by using the indicator "FOIA–APPEAL." Failure to address an appeal properly may delay commencement of the time limitation stated in paragraph (a)(1) of this section, to take account of the time reasonably required to forward the appeal to the Office of General Counsel.

§ 792.29 If I send NCUA confidential commercial information, can it be disclosed under FOIA?

(a) If you submit confidential commercial information to NCUA, it may be disclosed in response to a FOIA request in accordance with this section.

(b) For purposes of this section:

(1) *Confidential commercial information* means commercial or financial information provided to NCUA by a submitter that arguably is protected from disclosure under § 792.11(a)(4) because disclosure could reasonably be expected to cause substantial competitive harm.

(2) *Submitter* means any person or entity who provides business information, directly or indirectly, to NCUA.

(c) Submitters of business information must use good faith efforts to designate, by appropriate markings, either at the time of submission or at a reasonable time thereafter, those portions of their submissions deemed to be protected from disclosure under § 792.11(a)(4). Such a designation shall expire ten years after the date of submission.

(d) We will provide a submitter with written notice of a FOIA request or administrative appeal encompassing designated business information when:

(1) The information has been designated in good faith by the submitter as confidential commercial information deemed protected from disclosure under § 792.11(a)(4); or

(2) NCUA has reason to believe that the information may be protected from disclosure under § 792.11(a)(4).

Subject Index

E

F

I

L

M

T

U

V

NATIONAL CREDIT UNION ADMINISTRATION

12 CFR Part 701

Loans to Members and Lines of Credit to Members

AGENCY: National Credit Union Administration (NCUA).

ACTION: Final rule.

SUMMARY: NCUA is amending three subsections of its lending rule and this final rule clarifies: the conditions for applying the rule to loans secured by mobile homes, recreational vehicles, house trailers and boats; that loans secured by manufactured homes may be considered residential real estate loans; and that loans with a partial government guarantee, insurance, or advance commitment to purchase a portion of a loan fall within the rule. The changes incorporate legal interpretations previously issued by its Office of General Counsel (OGC) regarding permissible maturities for certain types of loans and the effect of partial government guarantees. The NCUA Board is making these changes because it believes it is helpful to federal credit unions (FCUs) and others that may consult NCUA regulations to incorporate these interpretations as part of the rule itself rather than having them stated separately in OGC legal opinions.

DATES: *Effective Date:* This rule is effective March 28, 2005.

FOR FURTHER INFORMATION CONTACT: Dianne M. Salva, Staff Attorney, Division of Operations, Office of General Counsel, at the above address or telephone: (703) 518–6540.

SUPPLEMENTARY INFORMATION:

Background

The Federal Credit Union Act (the FCU Act) generally limits an FCU's authority on matters of loan maturity, rates of interest, security and prepayment penalties. 12 U.S.C. 1757(5). As permitted under the FCU Act, the NCUA Board (the Board) has promulgated lending regulations allowing loan maturities of 20 years for mobile home loans and up to 40 years, or more with specific Board approval, on residential real estate loans. 12 CFR 701.21(f) and (g). NCUA's lending regulations also address loans secured by a state or federal government insurance or guarantee. 12 CFR 701.21(e). The OGC had recently issued several legal opinions addressing loan guarantees and loan maturities. In the course of the agency's annual review of regulations, the Board determined that the rules on loan guarantees and maturities should be updated to reflect the OGC opinions. Accordingly, on November 18, 2004, the Board issued a proposal to amend the lending regulations to incorporate the recent OGC opinions. 69 FR 68829, Nov. 26, 2004.

Summary of Comments

NCUA received eleven comments: five from state credit union leagues, two from national credit union trade organizations, three from individual credit unions, and one from a banking trade association. The comments were generally positive and supported the proposal to amend the regulation.

All of the comments that specifically addressed the proposed changes to § 701.21(e) of the rule regarding loan guarantees were favorable and supported the change. The final amendment to the rule, which is unchanged from the proposed, clarifies that a partial government guarantee, insurance, or commitment to purchase a loan is sufficient to effect the application of the regulation.

The majority of comments supported the proposed changes to § 701.21(f) and (g) regarding loan maturities for mobile homes, recreational vehicles and boats, and loan maturities for manufactured homes.

The banking trade association opposed the changes regarding loan maturities in whole, describing them as inconsistent with the credit union industry's specified mission of meeting the credit and savings needs of persons of modest means and arguing that they encourage unsafe lending practices. The Board disagrees. Rather, the Board finds that these amendments to the lending rule enhance an FCU's ability to meet the credit needs of its members. This rule allows FCUs to offer credit products that are more affordable to lower income members. Improvements in the quality and standards of construction of manufactured housing, for example, have resulted in increased values that may put the cost of shorter term loans out of the financial reach of individuals of modest means. The Board also disagrees that the longer maturities will encourage unsafe lending practices. To the contrary, as stated in the preamble to the proposed rule, NCUA encourages FCUs to take appropriate steps to ensure their liens are fully protected. Further, these changes to the regulation merely codify what OGC opinions have permitted for several years, and the Board is unaware of any evidence that the longer loan maturities have resulted in unsafe lending practices.

Two commenters raised issues revealing some confusion about the difference between mobile homes, which may have loan maturities up to 20 years, and manufactured homes, which are eligible for longer maturities. One FCU commented about a particular state law and local practices regarding the titling of manufactured housing as real or personal property, ground-leasing, and what constitutes ''permanently affixed,'' which, the commenter contended, could cause confusion and result in risks to FCUs making manufactured housing loans. In part, some confusion may result if the terms manufactured home and mobile home have a different meaning under a state law. In reviewing the FCU's letter, it became apparent that there may be issues under a state law that FCUs will need to address in their lending agreements with borrowers to ensure compliance with NCUA's lending regulation. One trade association suggested clarifying that manufactured housing that is not permanently affixed to the land constitutes a mobile home. The Board notes that, while this will generally be correct because a mobile home does not have to be permanently affixed to land, which is required for a manufactured home loan, a mobile home still must meet certain regulatory criteria to qualify for a maturity of up to 20 years.

The regulation distinguishes between mobile homes and manufactured homes. First, in using the term ''permanently affixed'' to describe manufactured homes as a type of manufactured housing distinguished from mobile homes, the Board intends to limit long-term loans to manufactured homes that are intended to remain in place permanently. In its opinion letter on this topic, the OGC stated:

> Most significantly, we note that a manufactured home, although constructed at a factory and not built on-site, is designed and intended to be permanently affixed to the land. Unlike a mobile home, which is also constructed at a factory, a manufactured home is not intended to be moved once it has reached its ultimate destination.

Legal Opinion OGC 03–0934, dated November 17, 2003. In order for a loan to qualify for the longer maturities of residential mortgage loans under § 701.21(g), a manufactured home must be designed and intended to remain in place permanently.

The same FCU noted above also commented about two issues regarding manufactured home loans discussed in the preamble to the proposed rule. Regarding the statement in the preamble that a manufactured home must qualify as real property and be titled as real

property, the FCU contends the requirement is unnecessary and that state law and local titling practices could cause problems. The Board notes that, for a loan to be eligible for a 30-year or more maturity term, the FCU Act requires that it be a ''residential *real estate* loan.'' 12 U.S.C. 1757(5)(A)(i) (emphasis added). Loans secured by some type of manufactured housing that is titled as personal property are not eligible for 30-year mortgages under the FCU Act but may be able to qualify as 20-year mobile home loans, assuming the criteria of § 701.21(f) are met. To the extent that a particular state law raises questions of how an FCU can ensure its loans comply with NCUA's lending regulation, an FCU may seek interpretive guidance from OGC.

Second, the FCU commented about the Board's suggestion that, for safety and soundness reasons, FCUs engaging in long-term loans for manufactured homes under § 701.21(g) should ensure, if the member is leasing the land where the manufactured home is located, that the term of the lease should be at least as long as the term of the loan. The FCU commented that this requirement is unnecessary and unreasonable, stating that, in practice, most manufactured housing communities permit leases of no longer duration than six months. First, the Board notes its statement in the preamble is not a regulatory requirement but is a statement of guidance. Second, the FCU's reference to a local practice of having short term leases of six months or less is a practice associated with mobile home parks rather than manufactured home locations. A manufactured home, as opposed to a mobile home, is designed and intended to stay in place permanently rather than be moved. The Board's understanding is that, in purchases of manufactured homes, the manufactured home is most often located on land the borrower already owns or is purchasing in conjunction with the purchase of the manufactured home. As noted in the preamble for the proposed rule, as a matter of safety and soundness, an FCU making a manufactured home loan where the land is leased should ensure that the lease is as long as the term of the loan. There may be some rare set of circumstances that would support an FCU making a 30-year loan on a manufactured home located on property that is leased for some lesser period of time. However, where the lease on land is of such a short duration that it places the loan security at a high risk of loss or waste, safety and soundness considerations would weigh against making a 30-year or more loan.

For these reasons, the Board has determined to adopt the proposed rule as a final rule with no changes.

Regulatory Procedures

Regulatory Flexibility Act

The Regulatory Flexibility Act (RFA) requires NCUA to prepare an analysis to describe any significant economic impact any regulation may have on a substantial number of small entities. NCUA considers credit unions having less than ten million in assets to be small for purposes of RFA. Interpretive Ruling and Policy Statement (IRPS) 87–2 as amended by IRPS 03–2. The rule clarifies and expands the lending rules to incorporate recent OGC opinions. NCUA has determined and certifies that this rule will not have a significant economic impact on a substantial number of small credit unions. Accordingly, NCUA has determined that a Regulatory Flexibility Analysis is not required.

Paperwork Reduction Act

NCUA has determined that the rule would not increase paperwork requirements under the Paperwork Reduction Act of 1995 and regulations of the Office of Management and Budget (OMB). NCUA currently has OMB clearance for § 701.21's collection requirements (OMB No. 3133–0139).

Executive Order 12612

Executive Order 12612 requires NCUA to consider the effect of its actions on state interests. This rule applies to only federally chartered credit unions. NCUA has determined that the final rule does not constitute a ''significant regulatory action'' for purposes of the Executive Order.

Executive Order 13132

Executive Order 13132 encourages independent regulatory agencies to consider the impact of their actions on state and local interests. In adherence to fundamental federalism principles, NCUA, an independent regulatory agency as defined in 44 U.S.C. 3502(5), voluntarily complies with the executive order. The rule applies only to federal credit unions. NCUA has determined that the amendments to the rule will not have a substantial direct effect on the states, on the connection between the national government and the states, or on the distribution of power and responsibilities among the various levels of government. NCUA has determined that this rule does not constitute a policy that has federalism implications for purposes of the executive order.

Small Business Regulatory Enforcement Fairness Act

The Small Business Regulatory Enforcement Fairness Act of 1996 (Pub. L. 104–121) provides generally for congressional review of agency rules. A reporting requirement is triggered in instances where NCUA issues a final rule as defined by Section 551 of the Administrative Procedures Act. 5 U.S.C. 551. NCUA submitted the rule to the Office of Management and Budget, which has determined that it is not major for purposes of the Small Business Regulatory Enforcement Fairness Act of 1996.

List of Subjects in 12 CFR Part 701

Credit unions, loans.

By the National Credit Union Administration Board on February 17, 2005.

Mary Rupp,

Secretary of the Board.

NATIONAL CREDIT UNION ADMINISTRATION

12 CFR Part 748

Security Program and Appendix B—Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice

AGENCY: National Credit Union Administration (NCUA).

ACTION: Final rule.

SUMMARY: NCUA is amending its rule governing security program elements to require federally insured credit unions to include response programs to address instances of unauthorized access to member information. NCUA is also including guidance, in the form of Appendix B, to provide federally insured credit unions with direction on ways to meet the new regulatory requirements.

DATES: This rule is effective on June 1, 2005.

FOR FURTHER INFORMATION CONTACT: Matthew J. Biliouris, Senior Information Systems Officer, Office of Examination & Insurance, Division of Supervision, at telephone (703) 518–6394; or Ross Kendall, Staff Attorney, Office of General Counsel, at telephone (703) 518–6562.

SUPPLEMENTARY INFORMATION: The contents of this preamble are listed in the following outline:

I. Introduction

In 2001, NCUA amended 12 CFR Part 748 to fulfill a requirement in Section 501 of the Gramm-Leach-Bliley Act (Pub. L. 106–102) (GLBA), in which Congress directed both NCUA and the other Federal Financial Institution Examination Council (FFIEC) agencies, including the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision (collectively, the ''Banking Agencies'') to establish standards for financial institutions relating to administrative, technical, and physical safeguards to: (1) Insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

Although NCUA worked with the Banking Agencies to develop the standards described above, the Banking Agencies issued their standards as guidelines under the authority of Section 39 of the Federal Deposit Insurance Act.

Since Section 39 of the Federal Deposit Insurance Act does not apply to NCUA, the NCUA Board determined that it could best meet the congressional directive to prescribe standards through an amendment to its existing regulation governing security programs for federally insured credit unions and by providing guidance to credit unions, substantially identical to the guidelines issued by the Banking Agencies, in an appendix to the regulation. 12 CFR Part 748, Appendix A; 66 FR 8152 (January 30, 2001). The preamble to the final rule discusses the different regulatory framework under which the Banking Agencies issued their guidelines. The final regulation requires each federally insured credit union to establish and maintain a security program implementing the safeguards required by GLBA.

Appendix A, entitled Guidelines for Safeguarding Member Information (Appendix A), is intended to outline industry best practices and assist credit unions to develop meaningful and effective security programs to ensure compliance with the requirements contained in the regulation. Among other things, Appendix A advises credit unions to: (1) Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of member information or member information systems; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of member information; and (3) assess the sufficiency of policies, procedures, member information systems, and other arrangements in place to control risks.[1]

On October 23, 2003, the NCUA Board approved a proposal to revise 12 CFR Part 748 to include a requirement to respond to incidents of unauthorized access to member information. The Board invited comment on all aspects of the proposed Guidance. The public comment period closed on December 29, 2003.

This final rule further amends Part 748 to require that every federally insured credit union have a security program that contains a provision for responding to incidents of unauthorized access to member information. Appendix B, entitled Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, is also provided to assist credit unions in developing and maintaining their response programs. Appendix B describes NCUA's expectation that every federally insured credit union develop a response program, including member notification procedures, to address unauthorized access to or use of member information that could result in substantial harm or inconvenience to a member.

NCUA has modified the proposed Guidance to provide credit unions with greater flexibility to design a risk-based response program tailored to the size, complexity and nature of its operations, while continuing to highlight member notice as a key feature of a credit union's response program. In addition, NCUA reorganized the proposed Guidance for greater clarity. A more detailed discussion of the changes follows.

II. Overview of Comments Received

NCUA received 15 comment letters on the proposed Guidance: Six from natural person credit unions, one from a corporate credit union, two from national credit union trade associations, five from state credit union leagues, and one from a service provider. In addition, the Banking Agencies collectively received 65 comment letters. While the NCUA Board carefully considered all comments on its proposed rule, to remain as consistent as practicable with the Banking Agencies, the Board has also made some changes in the final rule as a result of interagency discussions.

As a general matter, commenters agreed that credit unions should have response programs. Indeed, many credit unions and other financial institutions described having such programs in place. Many comments received commended the NCUA and the Banking Agencies for providing guidance on response programs. However, the majority of industry commenters criticized the prescriptive nature of the proposed Guidance. These commenters stated that the rigid approach in the proposed Guidance would stifle innovation and retard the effective evolution of response programs.

[1] 12 CFR Part 748, Appendix A, Paragraph III.B.2.

Industry commenters raised concerns that the specific requirements in the proposed Guidance would not permit a credit union to assess different situations from its own business perspective, specific to its size, operational and system structure, and risk tolerances.

Some industry commenters asserted that there is no need for regulation in this area and recommended that the NCUA and the Banking Agencies withdraw the proposed Guidance. Some of these commenters suggested, instead, that the Agencies re-issue the proposed Guidance as a best practices document. Other industry commenters suggested modifying the proposed Guidance to give credit unions greater discretion to determine how to respond to incidents of unauthorized access to or use of member information.

Two commenters also requested that the Agencies include a transition period allowing adequate time for financial institutions to implement the final Guidance. Some commenters asked for a transition period only for the aspects of the final Guidance that address service provider arrangements.

III. Overview of Final Guidance

The final rule requires that every federally insured credit union must develop and implement a response program designed to address incidents of unauthorized access to member information maintained by the credit union or its service provider. The final Guidance provides each credit union with greater flexibility to design a risk-based response program tailored to the size, complexity and nature of its operations.

The final Guidance, which has been reorganized for greater clarity, continues to highlight member notice as a key feature of a credit union's response program. However, in response to the comments received, the final Guidance modifies the standard describing when notice should be given and provides for a delay at the request of law enforcement. It also modifies which members should be given notice, what a notice should contain, and how it should be delivered.

A more detailed discussion of the final Guidance and the manner in which it incorporates comments NCUA and the Banking Agencies received follows.

IV. Section-by-Section Analysis of the Comments Received

A. The ''Background'' Section

Legal Authority

The legal foundation for the Guidance is set forth in Part 748, which derives from section 501(b) of GLBA and requires that every credit union have a security program. Appendix A to Part 748 describes the elements of a security program and includes measures to protect member information maintained by the credit union or its service providers. The Guidance states that NCUA expects member notification to be a component of such a response program.

One commenter questioned NCUA's and the Banking Agencies' legal authority to issue the Guidance. This commenter asserted that section 501(b) of GLBA only authorizes the Agencies to establish standards requiring financial institutions to safeguard the confidentiality and integrity of customer information and to protect that information from unauthorized access, but does not authorize standards that would require a response to incidents where the security of customer information actually has been breached.

The NCUA Board notes, however, that section 501(b)(3) specifically states that the standards to be established by the Agencies must include various safeguards to protect against not only ''unauthorized access to,'' but also, the ''use of'' customer information that could result in ''substantial harm or inconvenience to any customer.'' The NCUA Board determined that this language provides a legal basis for standards that include response programs to address incidents of unauthorized access to member information. Response programs represent the principal means for a credit union to protect against unauthorized ''use'' of member information that could lead to ''substantial harm or inconvenience'' to the member. For example, member notification is an important tool that enables a member to take steps to prevent identity theft, such as by arranging to have a fraud alert placed in his or her credit file.

Scope of Guidance

The proposed Guidance contained several cross references to definitions used in Appendix A. However, the NCUA Board did not specifically address the scope of the proposed Guidance. A number of commenters had questions and suggestions regarding the scope of the proposed Guidance and the meaning of terms used.

Entities and Information Covered

Some commenters had questions about the entities and information covered by the proposed Guidance. One commenter suggested that NCUA and the Banking Agencies clarify that foreign offices, branches, and affiliates of United States banks are not subject to the final Guidance. Another commenter wanted the NCUA Board to clarify corporate credit unions' responsibilities relating to the Guidance. This commenter wanted to know if corporate credit unions would be expected to follow the same practices of that of a service provider and notify affected natural person credit unions.

Some commenters recommended that the Agencies clarify that the final Guidance only applies to unauthorized access to sensitive information within the control of the financial institution. One commenter thought that the final Guidance should be broad and cover fraud committed against credit union members through the Internet, such as through the misuse of online corporate identities to defraud online banking users through fake web sites (commonly known as ''phishing''). Several commenters requested confirmation in the final Guidance that it applies to consumer accounts and not to business and other commercial accounts.

For greater clarity, NCUA has revised the Background section of the final Guidance to state that the scope and definitions of terms used in the Guidance are identical to those in section 501(b) of the GLBA and Appendix A, which largely cross-reference definitions used in NCUA's Privacy Rule.[2] Therefore, consistent with section 501(b) and Appendix A, this final Guidance applies to the entities enumerated in section 505(a) of the GLBA. This final Guidance does not apply to a credit union's foreign offices, branches, or CUSOs. However, a credit union is responsible for the security of its member information, whether the information is maintained within or outside of the United States, and whether or not it relies on a CUSO to provide certain member services.

As with the guidance contained in Appendix A, natural person credit unions that use corporate credit unions as their ''service providers'' will likely look to the final Guidance in overseeing their service provider arrangements with those corporate credit unions. Accordingly, there is no exemption for corporate credit unions that provide services to natural person credit unions as part of normal processing business.

The final Guidance also applies to ''member information,'' meaning any record containing ''nonpublic personal information'' (as that term is defined in section 716.3(n) of NCUA's Privacy rule) about a credit union's member, whether in paper, electronic, or other form, that

[2] 12 CFR Part 716.

is maintained by or on behalf of the institution.[3] Consequently, the final Guidance applies only to information that is within the control of the credit union and its service providers, and would not apply to information directly disclosed by a member to a third party, for example, through a fraudulent web site.

Moreover, the final Guidance does not apply to information involving business or commercial accounts. Instead, the final Guidance applies to nonpublic personal information about a ''member'' within the meaning of Appendix A, namely, a consumer who obtains a financial product or service from a credit union to be used primarily for personal, family, or household purposes, and who has a continuing relationship with the credit union.[4]

Effect of Other Laws

Several commenters requested NCUA and the Banking Agencies explain how the final Guidance interacts with additional and possibly conflicting state law requirements. Most of these commenters urged that the final Guidance expressly preempt state law. By contrast, one commenter asked the Agencies to clarify that a financial institution must also comply with additional state law requirements. In addition, some commenters asked that the final Guidance provide a safe harbor defense against class action law suits. They suggested that the safe harbor should cover any credit union that takes reasonable steps that regulators require to protect member information, but, nonetheless, experiences an event beyond its control that leads to the disclosure of member information.

These issues do not fall within the scope of this final Guidance. The extent to which section 501(b) of GLBA, Appendix A, and any related NCUA interpretations, such as this final Guidance, preempts state law is governed by Federal law, including the procedures set forth in section 507 of GLBA, 15 U.S.C. 6807.[5] Moreover, there is nothing in Title V of the GLBA that authorizes NCUA to provide credit unions with a safe harbor defense. Therefore, the final Guidance does not address these issues.

Organizational Changes in the ''Background'' Section

For the reasons described earlier, the Background section is adopted essentially as proposed, except that the latter part of the paragraph on ''Service Providers'' and the entire paragraph on ''Response Programs'' are incorporated into the introductory discussion of Section II. The NCUA Board believes that the Background section is now clearer, as it focuses solely on the statutory and regulatory framework upon which the final Guidance is based. Comments and changes with respect to the paragraphs that were relocated are discussed in the next section.

B. The ''Response Program'' Section

There are a number of differences between the discussion of Response Programs in the proposed and final Guidance. The introduction to section II of the proposed Guidance stated that a response program should be a key part of a credit union's information security program required under Part 748. It also described the importance of having a response program and of timely notification of members when warranted. Section II of the proposed Guidance contained four detailed paragraphs describing each of the four components that a response program should contain.

The introductory language in the final Guidance now emphasizes that a credit union's response program should be risk-based and describes the components of a response program in a less prescriptive manner. Section II in the final Guidance specifically states that a credit union should implement security measures, from among the itemized list in Appendix A, designed to prevent unauthorized access to or use of member information, such as by placing access controls on member information systems and conducting background checks[6] for employees who are authorized to access member information. It then states that NCUA expects every credit union to develop and implement a risk-based response program (another security measure enumerated in Appendix A) designed to address incidents of unauthorized access to member information that occur despite measures to prevent security breaches. The final Guidance also states that a response program should be a key part of a credit union's information security program.

This introductory paragraph is intended to make clear that, based upon the prevalence of identity theft in the United States,[7] every credit union should have a response program to be prepared to prevent and address attempts to gain unauthorized access to its member information. The Board's expectation that each credit union will develop a response program is consistent with the provision in Appendix A calling for each credit union to design an information security program to control ''identified risks'' stemming from ''reasonably foreseeable internal and external threats.''[8]

Service Provider Contracts

The Background section of the proposed Guidance elaborated on the specific provisions that a credit union's contracts with its service providers should contain. The proposed Guidance stated that a credit union's contract with its service provider should require the service provider to disclose fully to the credit union information related to any breach in security resulting in an unauthorized intrusion into the credit union's member information systems maintained by the service provider. It stated that this disclosure would permit a credit union to expeditiously implement its response program.

Several commenters on the proposed Guidance agreed that a credit union's contracts with its service providers should require the service provider to disclose fully to the credit union information related to any breach in security resulting in an unauthorized intrusion into the credit union's member information systems maintained by the service provider. However, many commenters suggested modifications to this provision.

The discussion of this aspect of a credit union's contracts with its service providers is in section II of the final Guidance. It has been revised as follows in response to the comments received.

Timing of Service Provider Notification

NCUA and the Banking Agencies received a number of comments regarding the timing of a service

[3] *See* 12 CFR Part 745, Appendix A, Paragraph I.C.2.c.

[4] *See* 12 CFR Part 748, Appendix A, Paragraph I.C.2.b.; 12 CFR Part 716.3(i).

[5] Section 507 provides that state laws that are ''inconsistent'' with the provisions of Title V, Subtitle A of the GLBA are preempted ''only to the extent of the inconsistency.'' State laws are ''not consistent'' if they offer greater protection than Subtitle A, as determined by the Federal Trade Commission, after consultation with the agency or authority with jurisdiction under Section 505(a) of either the person that initiated the complaint or that is the subject of the complaint. *See* 15 U.S.C. 6807.

[6] A footnote has been added to this section to make clear that credit unions should also conduct background checks of employees to ensure that the credit union does not violate 12 U.S.C. 1785(d), which prohibits an institution from hiring an individual convicted of certain criminal offenses or who is subject to a prohibition order under 12 U.S.C. 1786(g).

[7] See, for example, the Federal Trade Commission's Identity Theft Survey Report of September 2003,'' available at *http://www.ftc.gov/os/2003/09synovatereport.pdf* estimating that 10 million Americans were victims of identify theft in 2002.

[8] 12 CFR Part 748, Appendix A, Paragraph III.B. and III.C.

provider's notice to a credit union. One commenter suggested requiring service providers to report incidents of unauthorized access to credit unions within 24 hours after discovery of the incident.

In response to comments on the timing of a service provider's notice to a credit union, the final Guidance states that a credit union's contract with its service provider should require the service provider to take appropriate action to address incidents of unauthorized access to the credit union's member information, including notifying the credit union as soon as possible of any such incident, to enable the credit union to expeditiously implement its response program. The NCUA Board determined that requiring notice within 24 hours of an incident may not be practicable or appropriate in every situation, particularly where, for example, it takes a service provider time to investigate a breach in security. Therefore, the final Guidance does not specify a number of hours or days by which the service provider must give notice to the credit union.

Existing Contracts With Service Providers

Some commenters expressed concerns that they would have to rewrite their contracts with service providers to require the disclosure described in this provision. These commenters asked NCUA to grandfather existing contracts and to apply this provision only prospectively to new contracts. Many commenters also suggested that the final Guidance contain a transition period to permit credit unions to modify their existing contracts.

The NCUA Board has decided not to grandfather existing contracts or to add a transition period to the final Guidance because, as stated in the proposed Guidance, this disclosure provision is consistent with the obligations in Appendix A that relate to service provider arrangements and with existing guidance on this topic previously issued by NCUA.[9] In order to ensure the safeguarding of member information, credit unions that use service providers likely have already arranged to receive notification from the service providers when member information is accessed in an unauthorized manner. In light of the comments received, however, NCUA recognizes that there are credit unions that have not formally included such a disclosure requirement in their contracts. Where this is the case, the credit union should exercise its best efforts to add a disclosure requirement to its contracts and any new contracts should include such a provision.

Thus, the final Guidance adopts the discussion on service provider arrangements largely as proposed. To eliminate any ambiguity regarding the application of this section to foreign-based service providers, however, the final Guidance now makes clear that a covered credit union[10] should be capable of addressing incidents of unauthorized access to member information in member information systems maintained by its domestic and foreign service providers.[11]

Components of a Response Program

As described earlier, commenters criticized the prescriptive nature of proposed Section II that described the four components a response program should contain. The proposed Guidance instructed credit unions to design programs to respond to incidents of unauthorized access to member information by (1) assessing the situation; (2) notifying regulatory and law enforcement agencies; (3) containing and controlling the situation; and (4) taking corrective measures. The proposed Guidance contained detailed information about each of these four components.

The introductory discussion in this section of the final Guidance now makes clear that, as a general matter, a credit union's response program should be risk-based. It applies this principle by modifying the discussion of a number of these components. The NCUA Board determined that the detailed instructions in these components of the proposed Guidance, especially in the ''Corrective Measures'' section, would not always be relevant or appropriate. Therefore, the final Guidance describes, through brief, bulleted points, the elements of a response program, giving credit unions greater discretion to address incidents of unauthorized access to or use of member information that could result in substantial harm or inconvenience to a member.

At a minimum, a credit union's response program should contain procedures for (1) assessing the nature and scope of an incident, and identifying what member information systems and types of member information have been accessed or misused; (2) notifying the appropriate NCUA Regional Director and, in the case of state-chartered credit unions, its applicable state supervisory agency as soon as possible when the credit union becomes aware of an incident involving unauthorized access to or use of sensitive member information, as defined in the final Guidance, (3) immediately notifying law enforcement authorities in situations involving Federal criminal violations requiring immediate attention; (4) taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of member information, such as by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and (5) notifying members when warranted.

Assess the Situation

The proposed Guidance stated that a credit union should assess the nature and scope of the incident and identify what member information systems and types of member information have been accessed or misused.

Some commenters stated that NCUA and the Banking Agencies should retain this provision in the final Guidance. One commenter suggested that a credit union should focus its entire response program primarily on addressing unauthorized access to sensitive member information.

The NCUA Board has concluded that a credit union's response program should begin with a risk assessment that allows a credit union to establish the nature of any information improperly accessed. This will allow the credit union to determine whether and how to respond to an incident. Accordingly, the NCUA Board has not changed this provision.

Notify Regulatory and Law Enforcement Agencies

The proposed Guidance provided that a credit union should promptly notify NCUA when it becomes aware of an incident involving unauthorized access to or use of member information that could result in substantial harm or inconvenience to members. To clarify its expectations, the NCUA Board has amended the bullet point addressing notification of the regulator to include notification of the appropriate NCUA Regional Director, as well as any applicable state supervisory agency in the case of state-chartered credit unions.

In addition, the proposed Guidance stated that a credit union should file a Suspicious Activity Report (SAR), if required, in accordance with 12 CFR

[9] *See* FFIEC Information Technology Examination Handbook, Outsourcing Technology Services Booklet, June 2004; NCUA Letter to Credit Unions No. 00–CU–11, December 2000.

[10] *See* footnote 5, *supra.*

[11] *See e.g.*, FFIEC Information Technology Examination Handbook, Outsourcing Technology Services Booklet, June 2004.

Part 748 and various NCUA issuances.[12] The proposed Guidance stated that, consistent with the NCUA's SAR regulation, in situations involving Federal criminal violations requiring immediate attention, the credit union immediately should notify, by telephone, the appropriate law enforcement authorities and its primary regulator, in addition to filing a timely SAR. For the sake of clarity, the final Guidance discusses notice to regulators and notice to law enforcement in two separate, bulleted items.

Standard for Notice to Regulators

The provision regarding notice to regulators in the proposed Guidance prompted numerous comments. Many commenters suggested that NCUA adopt a narrow standard for notifying regulators. These commenters were concerned that notice to regulators, provided under the circumstances described in the proposed Guidance, would be unduly burdensome for credit unions, service providers, and regulators, alike.

Some of these commenters suggested that NCUA adopt the same standard for notifying regulators and members. These commenters recommended that notification occur when a credit union becomes aware of an incident involving unauthorized access to or use of ''sensitive member information,'' a defined term in the proposed Guidance that specified a subset of member information deemed by NCUA as most likely to be misused.

Other commenters recommended that the Agencies narrow this provision so that a credit union will inform a regulator only in connection with an incident that poses a significant risk of substantial harm to a significant number of its members, or only in a situation where substantial harm to members has occurred or is likely to occur, instead of when it could occur.

Other commenters who advocated the adoption of a narrower standard asked NCUA to take the position that filing an SAR constitutes sufficient notice and that notification of other regulatory and law enforcement agencies is at the sole discretion of the credit union. One commenter stated that it is difficult to imagine any scenario that would trigger the response program without requiring a SAR filing. Some commenters asserted that if NCUA believes a lower threshold is advisable for security breaches, it should amend Part 748.

By contrast, some commenters recommended that the standard for notification of regulators remain broad. One commenter advocated that any event that triggers an internal investigation by the credit union should require notice to the appropriate regulator. Another commenter similarly suggested that notification of all security events to federal regulators is critical, not only those involving unauthorized access to or use of member information that could result in substantial harm or inconvenience to its members.

The NCUA Board has concluded that the standard for notification to regulators should provide an early warning to allow NCUA or applicable state supervisory agency to assess the effectiveness of a credit union's response plan, and, where appropriate, to direct that notice be given to members if the credit union has not already done so. Thus, the standard in the final Guidance states that a credit union should notify its primary regulator as soon as possible if the credit union becomes aware of an incident involving unauthorized access to or use of ''sensitive member information.''

''Sensitive member information'' is defined in section III of the final Guidance and means a member's name, address, or telephone number, in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the member's account. ''Sensitive member information'' also includes any combination of components of member information that would allow someone to log onto or access the member's account, such as user name and password or password and account number.

This standard is narrower than that in the proposed Guidance because a credit union will need to notify NCUA when, and only if, it becomes aware of an incident involving ''sensitive member information.'' Therefore, under the final Guidance, there will be fewer occasions when a credit union should need to notify NCUA. However, under this standard, a credit union will need to notify NCUA at the time that the credit union initiates its investigation to determine the likelihood that the information has been or will be misused, so that NCUA will be able to take appropriate action, if necessary.

Notice to Regulators by Service Providers

Commenters on the proposed Guidance questioned whether a credit union or its service provider should give notice to a regulator when a security incident involves an unauthorized intrusion into the credit union's member information systems maintained by the service provider. One commenter noted that if a security event occurs at a large service provider, regulators could receive thousands of notices from institutions relating to the same event. The commenter suggested that if a service provider is examined by one of the Agencies the most efficient means of providing regulatory notice of such a security event would be to allow the servicer to notify its primary Agency contact. The primary Agency contact then could disseminate the information to the other regulatory agencies as appropriate.

The NCUA Board believes it is the responsibility of the credit union and not the service provider to notify NCUA. Therefore, the final Guidance states that a credit union should notify NCUA as soon as possible when the credit union becomes aware of an incident involving unauthorized access to or use of sensitive member information. Nonetheless, a security incident at a service provider could have an impact on multiple financial institutions that are supervised by different Federal regulators. Therefore, in the interest of efficiency and burden reduction, the last paragraph in section II of the final Guidance makes clear that a credit union may authorize or contract with its service provider to notify the NCUA on the credit union's behalf when a security incident involves an unauthorized intrusion into the credit union's member information systems maintained by the service provider.

Notice to Law Enforcement

Some commenters took issue with the provision in the proposed Guidance regarding notification of law enforcement by telephone. One interagency commenter asked the Banking Agencies to clarify how notification of law enforcement by telephone would work since in many cases it is unclear what telephone number should be used. This commenter maintained that size and sophistication of law enforcement authorities may differ from state to state and this requirement may create confusion and unwarranted action by the law enforcement authority.

The final Guidance adopts this provision as proposed. The NCUA

[12] *See* 12 CFR Part 748.1(c); NCUA Letter to Credit Unions No. 04–CU–03, Suspicious Activity Reports, March 2004; NCUA Regulatory Alert No. 04–RA–01, The Suspicious Activity Report (SAR) Activity Review—Trends, Tips, & Issues, Issue 6, November 2003, February 2004.

Board notes that the provision stating that a credit union should notify law enforcement by telephone in situations involving federal criminal violations requiring immediate attention is consistent with Part 748.

Contain and Control the Situation

The proposed Guidance stated that the credit union should take measures to contain and control a security incident to prevent further unauthorized access to or use of member information while preserving records and other evidence.[13] It also stated that, depending upon the particular facts and circumstances of the incident, measures in connection with computer intrusions could include: (1) Shutting down applications or third party connections; (2) reconfiguring firewalls in cases of unauthorized electronic intrusion; (3) ensuring that all known vulnerabilities in the credit union's computer systems have been addressed; (4) changing computer access codes; (5) modifying physical access controls; and (6) placing additional controls on service provider arrangements.

Few comments were received on this section. One interagency commenter suggested that the Banking Agencies adopt this section unchanged in the final Guidance. Another commenter had questions about the meaning of the phrase ''known vulnerabilities.'' Commenters did, however, note the overlap between proposed section II.C and the corrective measures in proposed section II.D, described as ''flagging accounts'' and ''securing accounts.''

NCUA and the Banking Agencies agree that some sections in the proposed Guidance overlapped. Therefore, the NCUA Board modified this section by incorporating concepts from the proposed Corrective Measures component, and removing the more specific examples in this section, including the terms that confused commenters. This section in the final Guidance gives a credit union greater discretion to determine the measures it will take to contain and control a security incident. It states that credit unions should take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of member information, such as, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence.

[13] *See* FFIEC Information Security Booklet, December. 2002, pp. 68–74, avaialble at *http://www.ffiec.gov/ffiecinfobase.html*__pages/it__01.htmlinfosec.

Preserving Evidence

One interagency commenter stated that the final Guidance should require financial institutions, as part of the response process, to have an effective computer forensics capability in order to investigate and mitigate computer security incidents as discussed in principle fourteen of the Basel Committee's ''Risk Management for Electronic Banking'' [14] and the International Organization for Standardization's ISO 17799.[15]

The NCUA Board notes that the final Guidance addresses not only computer security incidents, but also all other incidents of unauthorized access to member information. Thus, the Board thinks it is not appropriate to include more detail about steps a credit union should take to investigate and mitigate computer security incidents. However, the NCUA Board believes that credit unions should be mindful of industry standards when investigating an incident. Therefore, the final Guidance contains a reference to forensics by generally noting that a credit union should take appropriate steps to contain and control an incident, while preserving records and other evidence.

Corrective Measures

The proposed Guidance stated that once a credit union understands the scope of the incident and has taken steps to contain and control the situation, it should take measures to address and mitigate the harm to individual members. It then described three corrective measures that a credit union should include as a part of its response program in order to effectively address and mitigate harm to individual members: (1) Flagging accounts; (2) securing accounts; and (3) notifying members. The NCUA Board removed the first two corrective measures for the reasons that follow.

Flagging and Securing Accounts

The first corrective measure in the proposed Guidance directed credit unions to ''flag accounts.'' It stated that a credit union should immediately begin identifying and monitoring the accounts of those members whose information may have been accessed or misused. It also stated that a credit union should provide staff with instructions regarding the recording and reporting of any unusual activity, and if indicated given the facts of a particular incident, implement controls to prevent the unauthorized withdrawal or transfer of funds from member accounts.

The second corrective measure directed credit unions to ''secure accounts.'' The proposed Guidance stated that when a share draft, savings, or other member account number, debit or credit card account number, personal identification number (PIN), password, or other unique identifier has been accessed or misused, the credit union should secure the account and all other accounts and services that can be accessed using the same account number or name and password combination. The proposed Guidance stated that accounts should be secured until such time as the credit union and the member agree on a course of action.

Commenters were critical of these proposed measures. Several commenters asserted that the final Guidance should not prescribe responses to security incidents with this level of detail. Other commenters recommended that if NCUA chooses to retain references to ''flagging'' or ''securing'' accounts, it should include the words ''where appropriate'' in order to give credit unions the flexibility to choose the most effective solutions to problems.

Commenters also stated that the decision to flag accounts, the nature of the flag, and the duration of the flag, should be left to an individual credit union's risk-based procedures developed under Appendix A. These commenters asked NCUA to recognize that regular, ongoing fraud prevention and detection methods employed by a credit union may be sufficient.

Commenters representing small credit unions stated that they do not have the technology or other resources to monitor individual accounts. They stated that the financial impact of having to monitor accounts for unusual activity would be enormous, as each credit union would have to purchase expensive technology, hire more personnel, or both. These commenters asked NCUA to provide credit unions with the flexibility to close an account if the credit union detects unusual activity.

With respect to ''securing accounts,'' several commenters stated that if ''secure'' means close or freeze, either is extreme and would have significant adverse consequences for members. Other commenters stated that the requirement that the credit union and the member ''agree on a course of action'' is unrealistic, unworkable and should be eliminated. Some commenters explained that if a member is traveling and the credit union cannot contact the member to obtain the member's consent, freezing or closing a

[14] *http://www.bis.org/publ/bcbs35.htm.*

[15] *http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html.*

member's account could strand the member with no means of taking care of expenses. They stated that, in the typical case, the credit union would monitor such an account for suspicious transactions.

As described earlier, the NCUA Board is adopting an approach in the final Guidance that is more flexible and risk-based than that in the proposed Guidance. The final Guidance incorporates the general concepts described in the first two corrective measures into the brief bullets describing components of a response program enumerated in section II.C. Therefore, the first and second corrective measures no longer appear in the Guidance.

Member Notice and Assistance

The third corrective measure in the proposed Guidance is titled ''Member Notice and Assistance.'' This proposed measure stated that a credit union should notify and offer assistance to members whose information was the subject of an incident of unauthorized access or use under the circumstances described in section III of the proposed Guidance. The proposed Guidance also described which members should be notified. In addition, this corrective measure contained provisions discussing delivery and contents of the member notice.

The final Guidance now states that a credit union's response program should contain procedures for notifying members when warranted. For clarity's sake, the discussion of which members should be notified, and the delivery and contents of member notice, is now in new section III, titled ''Member Notice.'' Comments and changes with respect to the paragraphs that were relocated are discussed under the section titled ''Member Notice'' that follows.

Responsibility for Notice to Members

Some commenters were confused by the discussion in the proposed Guidance stating that a credit union's contract with its service provider should require the service provider to disclose fully to the credit union information related to any breach in security resulting in an unauthorized intrusion into the credit union's member information systems maintained by the service provider. Commenters stated that this provision appears to create an obligation for both credit unions and their service providers to provide notice of security incidents to the credit union's members. These commenters recommended that the service provider notify its credit union customer so that the credit union can provide appropriate notice to its members. Thus, members would avoid receiving multiple notices relating to a single security incident.

Other commenters asserted that a credit union should not have to notify its members if an incident has occurred because of the negligence of its service provider. These commenters recommended that in this situation, the service provider should be responsible for providing notice to the credit union's members.

As discussed above in connection with notice to regulators, the NCUA Board believes that it is the responsibility of the credit union, and not of the service provider, to notify the credit union's members in connection with an unauthorized intrusion into a credit union's member information systems maintained by the service provider. The responsibility to notify members remains with the credit union whether the incident is inadvertent or due to the service provider's negligence. The NCUA Board notes that the costs of providing notice to the credit union's members as a result of negligence on the part of the service provider may be addressed in the credit union's contract with its service provider.

The last paragraph in section II of the final Guidance, therefore, states that it is the responsibility of the credit union to notify the credit union's members. It also states that the credit union may authorize or contract with its service provider to notify members on the credit union's behalf when a security incident involves an unauthorized intrusion into the credit union's member information systems maintained by the service provider.

C. The ''Member Notice'' Section

Section III of the proposed Guidance described the standard for providing notice to members and defined the term ''sensitive member information'' used in that standard. This section also gave examples of circumstances when a credit union should give notice and when NCUA does not expect a credit union to give notice. It also discussed contents of the notice and proper delivery.

Section III of the final Guidance contains a more comprehensive discussion of member notice. It describes the standard for providing notice to members and defines both the terms ''sensitive member information'' and ''affected members.'' It also discusses the contents of the notice and proper delivery.

Standard for Providing Notice

A key feature of the proposed Guidance was the description of when a credit union should provide member notice. The proposed Guidance stated that a credit union should notify affected members whenever it becomes aware of unauthorized access to ''sensitive member information'' unless the credit union, after an appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected members, including by monitoring affected members' accounts for unusual or suspicious activity.

The NCUA Board proposed this standard as a way to strike a balance between notification to members every time the mere possibility of misuse of member information arises from unauthorized access and a situation where the credit union knows with certainty that information is being misused. However, the Board specifically requested comment on whether this is the appropriate standard and invited commenters to offer alternative thresholds for member notification.

Some commenters stated that the proposed standard was reasonable and sufficiently flexible. However, many commenters recommended that the Board provide credit unions with greater discretion to determine when a credit union should notify its members. Some of these commenters asserted that a credit union should not have to give notice unless the credit union believes it ''to be reasonably likely,'' or if circumstances indicated ''a significant risk'' that the information will be misused.

Commenters maintained that because the proposed standard states that a credit union should give notice when fraud or identity theft is merely possible, notification under these circumstances would needlessly alarm members where little likelihood of harm exists. Commenters claimed that, eventually, frequent notices in non-threatening situations will be perceived by members as routine and commonplace, and therefore reduce their effectiveness.

The NCUA Board believes that articulating as part of the Guidance a standard that sets forth when notice to members is warranted is both helpful and appropriate. However, the Board agrees with commenters and is concerned that the proposed threshold inappropriately required credit unions to prove a negative proposition, namely, that misuse of the information accessed

is unlikely to occur. In addition, the Board does not want members of credit unions to receive notices that would not be useful to them. Therefore, the NCUA Board has revised the standard for members notification.

The final Guidance provides that when a credit union becomes aware of an incident of unauthorized access to sensitive member information, the credit union should conduct a reasonable investigation to determine promptly the likelihood that the information has been or will be misused. If the credit union determines that misuse of the information has occurred or is reasonably possible, it should notify affected members as soon as possible.

An investigation is an integral part of the standard in the final Guidance. A credit union should not forego conducting an investigation to avoid reaching a conclusion that member information has been or will be misused and cannot unreasonably limit the scope of the investigation. However, the NCUA Board acknowledges that a full-scale investigation may not be necessary in all cases, such as where the facts readily indicate that information will or will not be misused.

Monitoring for Suspicious Activity

The proposed Guidance stated that a credit union need not notify members if it reasonably concludes that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected members, including by monitoring affected members' accounts for unusual or suspicious activity. A number of comments addressed the standard in the proposed Guidance on monitoring affected members' accounts for unusual or suspicious activity.

Some commenters stated that the final Guidance should grant credit unions the discretion to monitor the affected member accounts for a period of time and to the extent warranted by the particular circumstances. Some commenters suggested that monitoring occur during the investigation. One commenter noted that a credit union's investigation may reveal that monitoring is unnecessary. One commenter noted that monitoring the member's accounts at the credit union may not protect the member, because unauthorized access to member information may result in identity theft beyond the accounts held at the specific credit union.

The NCUA Board agrees that under certain circumstances, monitoring may be unnecessary, for example when, on the basis of a reasonable investigation, a credit union determines that information was not misused. The Board also agrees that the monitoring element may not protect the member. Indeed, an identity thief with unauthorized access to certain sensitive member information likely will open accounts at other financial institutions in the member's name.

Accordingly, the Board concludes that monitoring under the circumstances described in the standard for notice would be burdensome for credit unions without a commensurate benefit to members. For these reasons, the Board has removed the reference to monitoring in the final Guidance.

Timing of Notice

The proposed Guidance did not include specific language on the timing of notice to members, and NCUA and the Banking Agencies received many comments on this issue. Some commenters requested clarification of the time frame for member notice. One commenter recommended that NCUA adopt the approach in the proposed Guidance because it does not set forth any circumstances that may delay notification of the affected members. Another commenter maintained that, in light of a member's need to act expeditiously against identity theft, an outside limit of 48 hours after the credit union learns of the breach is a reasonable and timely requirement for notice to members. Many commenters, however, recommended that NCUA make clear that a credit union may take the time it reasonably needs to conduct an investigation to assess the risk resulting from a security incident.

The NCUA Board has responded to these various comments on the timing of notice by providing that a credit union notify an affected member ''as soon as possible'' after concluding that misuse of the member's information has occurred, or is reasonably possible. As the scope and timing of a credit union's investigation is dictated by the facts and circumstances of a particular case, the Board has not designated a specific number of hours or days by which credit unions should provide notice to members. The Board believes that doing so may inhibit a credit union's ability to investigate adequately a particular incident or may result in notice that is not timely.

Delay for Law Enforcement Investigation

The proposed Guidance did not address delay of notice to members while a law enforcement investigation is conducted. Many commenters recommended permitting a credit union to delay notification to members to avoid compromising a law enforcement investigation. These commenters noted that the California Database Protection Act of 2003 (CDPA) requires notification of California residents whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[16] However, the CDPA permits a delay in notification if a law enforcement agency determines that the notification will impede a criminal investigation.[17] Another commenter suggested that a credit union should not have to obtain a formal determination from a law enforcement agency before it is able to delay notice.

The NCUA Board agrees that it is appropriate to delay member notice if such notice will jeopardize a law enforcement investigation. However, to ensure that such a delay is necessary and justifiable, the final Guidance states that member notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the credit union with a written request for the delay.[18]

The NCUA Board is concerned that a delay of notification for a law enforcement investigation could interfere with the ability of members to protect themselves from identity theft and other misuse of their sensitive information. Thus, the final Guidance also provides that a credit union should notify its members as soon as notification will no longer interfere with the investigation and should maintain contact with the law enforcement agency that has requested a delay, in order to learn, in a timely manner, when member notice will no longer interfere with the investigation.

Sensitive Member Information

Scope of Standard

The Banking Agencies received many comments on the limitation of notice in the proposed Guidance to incidents involving unauthorized access to sensitive customer information. The NCUA Board invited comment on whether to modify the proposed standard for notice to apply to other circumstances that compel a credit union to conclude that unauthorized access to information, other than sensitive member information, likely

[16] The CDPA, also known as CA S.B. 1386, amended the Information Practices Act of 1977, California Civil Code, section 1798.82.

[17] *See* California Civil Code, section 1798.29(c).

[18] This includes circumstances when a credit union confirms that an oral request for delay from law enforcement will be followed by a written request.

will result in substantial harm or inconvenience to the affected members.

Most commenters recommended that the standard remain as proposed rather than covering other types of information. One interagency commenter suggested that the Agencies continue to allow a financial institution the discretion to notify affected customers in any other extraordinary circumstances that compel it to conclude that unauthorized access to information other than sensitive customer information likely will result in substantial harm or inconvenience to those affected. However, the commenter did not provide any examples of such extraordinary circumstances.

The NCUA Board continues to believe that the rationale for limiting the standard to sensitive member information expressed in the proposed Guidance is correct. The proposed Guidance explained that, in accordance with Appendix A, a credit union must protect against unauthorized access to or use of member information that could result in substantial harm or inconvenience to a member. Substantial harm or inconvenience is most likely to result from improper access to sensitive member information because this type of information is easily misused, as in the commission of identity theft.

The NCUA Board has not identified any other circumstances that should prompt member notice and continues to believe that it is not likely that a member will suffer substantial harm or inconvenience from unauthorized access to other types of information. Therefore, the standard in the final Guidance continues to be limited to unauthorized access to sensitive member information. Of course, a credit union still may send notices to members in any additional circumstances that it determines are appropriate.

Definition of Sensitive Member Information

NCUA received many comments on the proposed definition of ''sensitive member information'' in the proposed Guidance. The first part of the proposed definition stated that ''sensitive member information'' is a member's social security number, personal identification number (PIN), password or account number, in conjunction with a personal identifier such as the member's name, address, or telephone number. The second part of the proposed definition stated that ''sensitive member information'' includes any combination of components of member information that allow someone to log onto or access another person's account, such as user name and password.

Some commenters agreed with this definition of ''sensitive member information.'' They said that it was sound, workable, and sufficiently detailed. However, many commenters proposed additions, exclusions, or alternative definitions.

Additional Elements

Some commenters suggested that NCUA add various data elements to the definition of sensitive member information, including: A driver's license number or number of other government-issued identification, mother's maiden name, and date of birth. One commenter suggested inclusion of other information that credit unions maintain in their member information systems such as a member's account balance, account activity, purchase history, and investment information. The commenter noted that misuse of this information in combination with a personal identifier can just as easily result in substantial harm or inconvenience to a member.

The NCUA Board has added to the first part of the definition several more specific components, such as driver's license number and debit and credit card numbers, because this information is commonly sought by identity thieves. However, the Board determined that the second part of the definition would cover the remaining suggestions. For example, where date of birth or mother's maiden name are used as passwords, under the final Guidance they will be considered components of member information that allow someone to log onto or access another person's account. Therefore, these specific elements have not been added to the definition.

Exclusions

Commenters also asserted that the proposed definition of sensitive member information is too broad and proposed various exclusions. For example, some commenters asked NCUA to exclude publicly available information, and also suggested that the final Guidance apply only to account numbers for transaction accounts or other accounts from which withdrawals or transfers can be initiated. These commenters explained that access to a mortgage account number (which may also be a public record) does not permit withdrawal of additional funds or otherwise damage the member. Other commenters requested that NCUA exclude encrypted information. Some of these commenters noted that only unencrypted information is covered by the CDPA.[19]

The final Guidance does not adopt any of the proposed exclusions. The NCUA Board believes it would be inappropriate to exclude publicly available information from the definition of sensitive member information, where publicly available information is otherwise covered by the definition of ''member information.'' [20] So for instance, while a personal identifier, *i.e.,* name, address, or phone number, may be publicly available, it is sensitive member information when linked with particular nonpublic information such as a credit card account number. However, where the definition of ''member information'' does not cover publicly available information, sensitive member information also would not cover publicly available information. For instance, where an individual's name or address is linked with a mortgage loan account number that is in the public record, and therefore, would not be considered ''member information,'' [21] it also would not be considered sensitive member information for purposes of the final Guidance.

In addition, access to a member's personal information and account number, whether or not it is an account from which withdrawals or transfers can be initiated, may permit an identity thief to access other accounts from which withdrawals can be made. Thus, the NCUA Board has determined that the definition of account number should not be limited as suggested by commenters. The Board also believes that a blanket exclusion for all encrypted information is not appropriate, because there are many levels of encryption, some of which do not effectively protect member information.

Alternative Definitions

Most alternative definitions suggested by commenters resembled the definition of ''personal information'' under the CDPA.[22] Under the CDPA, ''personal information'' includes a resident of California's name together with an account number, or credit or debit card

[19] *See* California Civil Code, 1798.29(a).

[20] *See* 12 CFR Part 748, Appendix A, Paragraph I.C.2.c.

[21] *See* 12 CFR § 716.3(p)(3)(i).

[22] Under the California law requiring notice, ''personal information'' means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number; (2) driver's license number or California Identification Card number; (3) Account number, credit or debit card number, in combination with any required security code access code, or password that would permit access to an individual's financial account.

number only if the information accessed also includes any required security code, access code, or password that would permit access to an individual's financial account. Therefore, some commenters asked that the final Guidance clarify that a name and an account number, together, is not sensitive member information unless these elements are combined with other information that permits access to a member's financial account.

The NCUA Board concluded that it would be helpful if credit unions could more easily compare and contrast the definition of ''personal information'' under the CDPA with the definition of ''sensitive information'' under the final Guidance. Therefore, the elements in the definition of sensitive information in the final Guidance are re-ordered and the Board added the elements discussed earlier.

The final Guidance states that sensitive member information means a member's name, address, or telephone number, in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the member's account. The final Guidance also states that sensitive member information includes any combination of components of member information that would allow someone to log onto or access the member's account, such as user name and password or a password and account number.

Consistent with the Banking Agencies, the NCUA Board declines to adopt the CDPA standard for several reasons. First, for example, under the CDPA, personal information includes a person's name in combination with other data elements. By contrast, the final Guidance treats address and telephone number in the same manner as a member's name, because reverse directories may permit an address or telephone number to be traced back to an individual member.

In addition, under the CDPA, ''personal information'' includes name together with an account number, or credit or debit card number only if the information accessed also includes any required security code, access code, or password that would permit access to an individual's financial account. The NCUA Board notes that a name and account number, alone, is sufficient to create fraudulent checks, or to direct the unauthorized debit of a member's account even without an access code.[23] Further, a name and credit card number may permit unauthorized access to a member's account. Therefore, the final Guidance continues to define a member's name and account number, or credit or debit card number as sensitive member information.

Affected Customers

The NCUA Board also reviewed many interagency comments on the definition of ''affected members'' in the proposed Guidance. Section II.D.3 of the proposed Guidance provided that if the credit union could determine from its logs or other data precisely which members' information was accessed or misused, it may restrict its notification to those individuals. However, if the credit union cannot identify precisely which members were affected, it should notify each member in any group likely to have been affected, such as each member whose information is stored in the group of files in question.

Commenters were concerned that this provision in the proposed Guidance was overly broad. These commenters stated that providing notice to all members in groups likely to be affected would result in many notices that are not helpful. The commenters suggested that the final Guidance narrow the standard for notifying members to only those members whose information has been or is likely to be misused.

The discussion of ''affected members'' has been relocated and is separately set forth following the definition of ''sensitive member information'' in the final Guidance. The discussion of ''affected members'' in the final Guidance states that if a credit union, based upon its investigation, can determine from its logs or other data precisely which member's information has been improperly accessed,[24] it may notify only those members with respect to whom the credit union determines that misuse of their information has occurred or is reasonably possible. However, the final Guidance further notes that there may be situations where the credit union determines that a group of files has been accessed improperly, but is unable to identify which specific member's information has been accessed. If the circumstances of the unauthorized access lead the credit union to determine that misuse of the information contained in the group of files is reasonably possible, it should notify all members in the group. In this way, the final Guidance reduces the number of notices that should be sent.

Examples

The proposed Guidance described several examples of when a credit union should give notice and when NCUA does not expect a credit union to give notice.

NCUA received a number of comments on the examples. Some commenters thought the examples were helpful and suggested that NCUA add more. Other commenters criticized the examples as too broad. Many commenters suggested numerous ways to modify and clarify the examples.

Since the examples in the proposed Guidance led to interpretive questions, rather than interpretive clarity, the NCUA Board concluded that it is not particularly helpful to offer examples of when notice is and is not expected. In addition, the Board believes that the standard for notice itself has been clarified and examples are no longer necessary. Therefore, there are no examples in the final Guidance.

Content of Member Notice

NCUA received many comments on the discussion of the content of member notice located in section II.D.3.b of the proposed Guidance. The proposed Guidance stated that a notice should describe the incident in general terms and the member's information that was the subject of unauthorized access or use. It stated that the notice should also include a number that members can call for further information and assistance, remind members of the need to remain vigilant over the next 12 to 24 months, and recommend that members promptly report incidents of suspected identity theft. The proposed Guidance described several ''key elements'' that a notice should contain. It also provided a number of ''optional elements'' namely, examples of additional assistance that financial institutions have offered.

Some commenters agreed that the proposed Guidance sufficiently addressed most of the key elements necessary for an effective notice. However, many commenters requested greater discretion to determine the content of the notices that credit unions provide to members. Commenters suggested that NCUA make clear that the various items suggested for inclusion in any member notice are

[23] *See, e.g.,* Griff Witte, *Bogus Charges, Unknowingly Paid: FTC Accuses 2 of Raiding 90,000 Bank Accounts in Card Fraud,* Washington Post, May 29, 2004, at E1 (list of names with associated checking account numbers used by bogus company to debit bank accounts without customer authorization).

[24] NCUA notes that system logs may permit a credit union to determine precisely which members' data has been improperly accessed. *See, e.g.,* FFIEC Information Security Booklet, page 64, available at *http://www.ffiec.gov/ffiecinfobase.html*__pages/it__01.html‌infosec.

suggestions, and that not every item is mandatory in every notice.

Some commenters took issue with the enumerated items in the proposed Guidance identified as key elements that a notice should contain. For example, many commenters asserted that members should not necessarily be encouraged to place fraud alerts with credit bureaus in every circumstance. Some of these commenters noted that not all situations will warrant having a fraud alert posted to the member's credit file, especially if the credit union took appropriate action to render the information accessed worthless. According to these commenters, the consequences of a fraud alert, such as increased obstacles to obtaining credit, may outweigh any benefit. Some commenters also noted that a proliferation of fraud alerts not related to actual fraud would dilute the effectiveness of the alerts.

Other commenters criticized the optional elements in the proposed Guidance. For instance, some commenters stated that a notice should not inform the member about subscription services that provide notification to the member when there is a request for the member's credit report, or offer to subscribe the member to this service, free of charge, for a period of time. These commenters asserted that member notices should not be converted into a marketing opportunity for subscription services provided by consumer credit bureaus. They stated that offering the service may mislead the member into believing that these expensive services are essential. If the service is offered free of charge, a credit union's choice of service could be interpreted as an endorsement for a specific company and its product.

As a result of the Fair and Accurate Credit Transactions Act of 2003, Public Law 108–159, 117 Stat. 1985–86 (the FACT Act), many of the descriptions of ''key elements'' and ''optional elements'' in the proposed Guidance, and comments on these elements, have been superceded. For example, the frequency and circumstances under which a member may obtain a credit report free-of-charge have changed.

The final Guidance continues to specify that a notice should describe the incident in general terms and the member's information that was the subject of unauthorized access or use. It also continues to state that the notice should include a telephone number that members can call for further information and assistance, remind members of the need to remain vigilant over the next 12 to 24 months, and recommend that members promptly report incidents of suspected identity theft. In addition, the final Guidance also states that the notice should generally describe what the credit union has done to protect the members' information from further unauthorized access.

However, the final Guidance no longer distinguishes between certain other ''key'' items that the notice should contain and those that are ''optional.'' The NCUA Board added greater flexibility to this section to accommodate any new protections afforded to consumers that flow from the FACT Act. Instead of distinguishing between items that the notice should contain and those that are optional, a credit union may now select those items that are appropriate under the circumstances, and that are compatible with the FACT Act. Of course, credit unions may incorporate additional information that is not mentioned in the final Guidance, where appropriate.

Coordination With Credit Reporting Agencies

A trade association representing credit reporting agencies commented that its members are extremely concerned about their ability to comply with all of the duties (triggered under the FACT Act) that result from notices financial institutions send to their customers. This commenter strongly recommended that until a financial institution has contacted each nationwide consumer reporting agency to coordinate the timing, content, and staging of notices as well as the placement of fraud alerts, as necessary, a financial institution should refrain from issuing notices suggesting that customers contact nationwide consumer reporting agencies.

The commenter also stated that a financial institution that includes such suggestions in a notice to its customers should work with the credit reporting agencies to purchase the services the financial institution believes are necessary to protect its customers. The commenter stated that the costs of serving the millions of consumers it projects will receive notices under the proposed Guidance cannot be borne solely by the nationwide consumer reporting agencies.

The commenter also noted that the State of California has provided clear guidance in connection with its law requiring notice and also suggested that coordination with consumer reporting agencies is vital to ensure that a consumer can in fact request a file disclosure in a timely manner. This commenter stated that similar guidance at the federal level is essential.

The NCUA Board believes that the final Guidance addresses this commenter's concerns in several ways. First, for the reasons described earlier, the standard for member notice in the final Guidance likely will result in credit unions sending fewer notices. Second, the final Guidance does not require credit unions to send notices suggesting that consumers contact the nationwide consumer reporting agencies, in every case. Credit unions can use their discretion to determine whether such information should be included in a notice.

It is clear, however, that member notice may prompt more consumer contacts with consumer reporting agencies, as predicted by the commenter. Therefore, the final Guidance encourages a credit union that includes in its notice contact information for nationwide consumer reporting agencies to notify the consumer reporting agencies in advance, prior to sending large numbers of such notices. In this way, the reporting agencies will be on notice that they may have to accommodate additional requests for the placement of fraud alerts, where necessary.

Model Notice

Some commenters stated that if mandatory elements are included in the final Guidance, NCUA should develop a model notice that incorporates all the mandated elements yet allows credit unions to incorporate additional information where appropriate. Given the flexibility that credit unions now have to craft a notice tailored to the circumstances of a particular incident, the NCUA Board believes that any single model notice will be of little use. Therefore, the final Guidance does not contain a model notice.

Other Changes Regarding the Content of a Notice

The general discussion of the content of a notice in the final Guidance states that credit unions should give member notice in a ''clear and conspicuous manner.'' In addition, the final Guidance adopts a commenter's suggestion that credit unions should generally describe what the credit union has done to protect a member's information from further unauthorized access so that a member can make decisions regarding the credit union's member service. This addition allows a member to take measures to protect his or her accounts that are not redundant or in conflict with the credit union's actions.

The final Guidance also states that notice should include a telephone

number that members can call for further information and assistance. The NCUA Board added a new footnote to this text, which explains that the credit union should ensure that it has reasonable policies and procedures in place, including trained personnel, to respond appropriately to member inquiries and requests for assistance.

Delivery of Customer Notice

NCUA received numerous suggestions regarding the delivery of member notice located in section II.D.3.a of the proposed Guidance. The proposed Guidance stated that member notice should be timely, clear, and conspicuous, and delivered in any manner that will ensure that the member is likely to receive it. The proposed Guidance provided several examples of proper delivery and stated that a credit union may choose to contact all members affected by telephone or by mail, or for those members who conduct transactions electronically, using electronic notice.

One interagency commenter representing a large bank trade association agreed that this was a correct standard. However, many other commenters recommended that if it costs an institution more than $250,000 to provide notice to customers, if the affected class of persons to be notified exceeds 500,000, or if an incident warrants large distributions of notices, the final Guidance should permit various forms of mass distribution of information, such as by postings on an Internet web page and in national or regional media outlets. Commenters explained that the CDPA contains such a provision.[25]

One commenter suggested that a credit union should only provide notice in response to inquiries. By contrast, other commenters stated that the final Guidance should make clear that general notice on a web site is inadequate and that credit unions should provide individual notice to members.

The NCUA Board determined that the provision in the proposed Guidance that notice be delivered in a ''timely, clear, and conspicuous'' manner already appears elsewhere in the Guidance and is unnecessary here.

The NCUA Board has decided not to include a provision in the final Guidance that permits notice through a posting on the web or through the media in order to provide notice to a specific number of members or where the cost of notice to individual members would exceed a specific dollar amount. The Board believes that the thresholds suggested by commenters would not be appropriate in every case, especially in connection with incidents involving smaller institutions. Therefore, the final Guidance states that member notice should be delivered in any manner that is designed to ensure that a member can reasonably be expected to receive it. This standard places the responsibility on the credit union to select a method to deliver notice that is designed to ensure that a member is likely to receive notice.

The final Guidance also provides examples of proper delivery, noting that a credit union may choose to contact all members affected by telephone or by mail, or by electronic mail for those members for whom it has a valid e-mail address and who have agreed to receive electronic communications from the credit union. Some commenters questioned the effect of other laws on the proposed Guidance. A few commenters noted that electronic notice should conform to the requirements of the Electronic Signatures in Global and National Commerce Act (E-Sign Act), 15 U.S.C. 7001 *et seq.* The final Guidance does not discuss a credit union's obligations under the E-Sign Act. The NCUA Board notes that the final Guidance specifically contemplates that a credit union may give notice electronically or by telephone. There is no requirement that notice be provided in writing. Therefore, the final Guidance does not trigger any consent requirements under the E-Sign Act.[26]

Still other commenters requested clarification that a telephone call made to a member for purposes of complying with the final Guidance is for ''emergency purposes'' under the Telephone Consumer Protection Act, 47 U.S.C. 227 (TCPA). These commenters noted that this is important because under the TCPA and its implementing regulation,[27] it is unlawful to initiate a telephone call to any residential phone line using an artificial or prerecorded voice to deliver a message, without the prior express consent of the called party, unless such call is for ''emergency purposes.''

The final Guidance does not address the TCPA, because the TCPA is interpreted by the Federal Communications Commission (FCC), and the FCC has not yet taken a position on this issue.[28]

V. Effective date

Many commenters suggested that NCUA include a transition period to allow adequate time for credit unions to implement the final Guidance. In accordance with applicable federal law, the final amendment to Part 748 is effective thirty days after publication in the **Federal Register**.

In addition, given the comments received, the NCUA Board recognizes that not every credit union currently has a response program that is consistent with the final Guidance. The Board expects these credit unions to implement the final Guidance as soon as possible. However, the Board appreciates that some credit unions may need additional time to develop new compliance procedures, modify systems, and train staff in order to implement an adequate response program. The NCUA Board will take into account the good faith efforts made by each credit union to develop a response program that is consistent with the final Guidance, together with all other relevant circumstances, when examining the adequacy of a credit union's information security program.

VII. Impact of Guidance

The NCUA Board invited comment on the potential burden associated with the member notice provisions for credit unions implementing the proposed Guidance. The Board also asked for information about the anticipated burden that may arise from the questions posed by members who receive the notices. In addition, the proposed Guidance asked whether NCUA should consider how the burden

[25] *See* CAL. CIV. CODE § 1798.82(g)(3) (West 2005).

[26] Under the E-Sign Act, if a statute, regulation, or other rule of law *requires* that information be provided or made available to a consumer in writing, certain procedures apply. *See* 15 U.S.C. 7001(c).

[27] 47 CFR 64.1200.

[28] NCUA notes, however, that the TCPA and its implementing regulations generally exempt calls made to any person with whom the caller has an established business relationship at the time the call is made. *See, e.g.,* 47 CFR 64.1200(a)(1)(iv). Thus, the TCPA would not appear to prohibit a credit union's telephone calls to its own members. In addition, the FCC's regulations state that the phrase for ''emergency purposes'' means calls made necessary in any situation affecting the health and safety of consumers. 47 CFR 64.1200(f)(2). *See also* FCC Report and Order adopting rules and regulations implementing the TCPA, October 16, 1992, available at *http://www.fcc.gov/cgb/donotcall/,* paragraph 51 (calls from utilites to notify customers of service outages, and to warn customers of discontinuance of service are included within the exemption for emergencies). Credit unions will give members notice under the final Guidance for a public safety purpose, namely, to permit their members to protect themselves where their sensitive information is likely to be misused, example, to facilitate identity theft. Therefore, the NCUA Board believes that the exemption for emergency purposes likely would include member notice that is provided by telephone using an artificial or prerecorded voice message call.

may vary depending upon the size and complexity of a credit union. The Board also asked for information about the amount of burden, if any, the proposed Guidance would impose on service providers.

Although many commenters representing credit unions stated that they already have a response program in place, they also noted that NCUA had underestimated the burden that would be imposed on credit unions and their members by the proposed Guidance. Some commenters stated that the proposed Guidance would require greater time, expenditure, and documentation for audit and compliance purposes. Other commenters stated that the costs of providing notice and requiring a sufficient number of appropriately trained employees to be available to answer member inquiries and provide assistance could be substantial. Other commenters stated that the Agencies failed to adequately consider the burden to members and customers who begin to receive numerous notices of ''unauthorized access'' to their data. They stated that the stress to members of having to change account numbers, change passwords, and monitor their credit reports would be enormous and could be unnecessary because the standard in the proposed Guidance would require notice when information subject to unauthorized access might be, but would not necessarily be, misused.

Some commenters maintained that the proposed Guidance would be especially burdensome for small credit unions, which one commenter asserted are the lowest risk targets. These commenters stated that the most burdensome elements of the proposed Guidance would be creating a general policy, establishing procedures and training staff. They added that developing and implementing new procedures for determining when, where and how to provide notice and procedures for monitoring accounts would also be burdensome.

Finally, a trade association commenter stated that the notice requirements in the proposed Guidance would impose a large burden on the nationwide consumer reporting agencies, over which they have no control and from which they have no means of recouping costs.

The NCUA Board has addressed the burdens identified by commenters as follows. First, the Board eliminated many of the more prescriptive elements of the response program described in the proposed Guidance. The final Guidance states that a credit union's response program should be risk-based. It lists a number of components that the program should contain.

Second, final Guidance does not detail the steps that a credit union should take to contain and control a security incident to prevent further unauthorized access to or use of member information. It also does not state that a credit union should secure all accounts that can be accessed using the same account number or name and password combination until such time as the credit union and the member can agree on a course of action. Instead, the final Guidance leaves such measures to the discretion of the credit union and gives examples of the steps that a credit union should consider, such as monitoring, freezing, or closing affected accounts. Thus, under the final Guidance a small credit union may choose to close an affected account, rather than monitoring the account, an element of the proposed Guidance that smaller credit unions identified as potentially very costly.

Third, though the final Guidance still states that notification to regulators should be a part of a credit union's response program, it states that notice should only be given when the credit union becomes aware of an incident of unauthorized access to or use of ''sensitive'' member information. This standard should result in fewer instances of notice to the regulators than under the proposed Guidance. The final Guidance also makes clear that when the security incident involves a service provider, the credit union may authorize the service provider to notify the credit union's regulator.

Fourth, the standard of notice to members also has been modified to be less burdensome to credit unions and their members. The NCUA Board believes that under this new standard, members will be less likely to be alarmed needlessly, and credit unions will no longer be asked to prove a negative—namely, that misuse of information is unlikely to occur. In addition, the Board also has provided credit unions with greater discretion to determine what should be contained in a notice to members.

The NCUA Board does not believe that there is a basis for exempting small credit unions from the Guidance. For example, many small credit unions outsource functions to large service providers that have been the target of those seeking to misuse member information. Therefore, the Board believes that all credit unions should prepare member response programs including member notification procedures that can be used in the event the credit union determines that misuse of its information about a member has occurred or is reasonably possible. However, as noted above, the Board recognizes that within the framework of the Guidance, a credit union's program will vary depending on the size and complexity of the credit union and the nature and scope of its activities.

Finally, to address comments relating to the potential burden on the nationwide consumer reporting agencies, as noted previously, the Guidance no longer suggests that member notice always include advice to contact the nationwide consumer reporting agencies. The NCUA Board recognizes that not all security breaches warrant such contacts. For example, the Board recognizes that it may not always be in the best interest of a consumer to have a fraud alert placed in the consumer's file because the fraud alert may have an adverse impact on the consumer's ability to obtain credit.

VIII. Regulatory Procedures

Paperwork Reduction Act

Certain provisions of the final Guidance contain ''collection of information'' requirements as defined in the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) (PRA). An agency may not conduct or sponsor, and a respondent is not required to respond to, an information collection unless it displays a currently valid Office of Management and Budget (OMB) control number.

The NCUA Board requested comment on a proposed information collection as part of the notice requesting comment on the proposed Guidance. An analysis of the comments related to paperwork burden and commenters' recommendations is provided below. The NCUA submitted its proposed information collection to OMB for review and approval and the collections have been approved.

The NCUA Board has reconsidered the burden estimates published in the Proposed Guidance in light of the comments received asserting that the paperwork burden associated with the information collection were underestimated, and in light of measures taken to reduce burden in this final Guidance. The Board agreed to increase the estimate for the time it will take a credit union to develop notices and determine which members should be notified. However, revisions incorporated into the final Guidance will result in the preparation and issuance of fewer notices than was originally estimated. Therefore, the net change in burden is due to the rounding of numbers. A discussion of the

comments received follows the revised estimates.

New Estimates

Number of Respondents: 9,014.
Estimated Time per Response:
Developing Notices: 24 hours x 9,014 = 216,336 hours.
Notifying Customers: 29 hours x 153 = 4,437 hours.

Total Estimated Annual Burden = 220,773 hours .

Discussion of Comments

The information collection in the proposed Guidance stated that credit unions should: (1) Develop notices to members; and (2) determine which members should receive the notices and send the notices to members. The NCUA Board and the Banking Agencies received various comments regarding the burden estimates, including the estimated time per response and the number of recordkeepers involved.

Some commenters stated that the burden estimates of twenty hours to develop and produce notices and three days to determine which members should receive notice in the proposed Guidance were too low. These commenters stated that the Guidance should include language indicating that a credit union be given as much time as necessary to determine the scope of an incident and examine which members may be affected. One of these commenters stated that ten business days, as recommended by the California Department of Consumer Affairs Office of Privacy Protection, should provide a credit union with a known safe harbor to complete the steps described lest regulated entities be subject to inconsistent notification deadlines from the same incident.

These commenters misunderstood the meaning of PRA burden estimates. PRA burden estimates are judgments by the NCUA regarding the length of time that it would take credit unions to comply with information collection requirements. These estimates do not impose a deadline upon credit unions to complete a requirement within a specific period of time.

The final Guidance states that a credit union should notify members ''as soon as possible'' after an investigation leads it to conclude that misuse of member information has occurred or is reasonably possible. It also states that notification may be delayed at the written request of law enforcement.

The cost of disclosing information is considered part of the burden of an information collection. 5 CFR 1320.3(b)(1)(ix). Many commenters stated that the Agencies had underestimated the cost associated with disclosing security incidents to members pursuant to the proposed Guidance. However, these commenters did not distinguish between the usual and customary costs of doing business and the costs of the disclosures associated with the information collection in the proposed Guidance.

For example, one commenter stated that the Agencies' estimate did not include $0.60 per member for a one-page letter, envelope, and first class postage; the customer service time, handling the enormous number of calls from customers who receive notice; or the costs associated with closing or reopening accounts, printing new checks or embossing new cards. This commenter stated that printing and mailing costs, alone, for one notice to its customer database, at current postal rates, would be at least $500,000.

Some of the costs mentioned in this comment are non-labor costs associated with providing disclosures. Both NCUA and the Banking Agencies assumed that non-labor costs associated with the disclosures would be negligible, because institutions already have in place well-developed systems for providing disclosures to their customers. This comment and any other comments received regarding the Agencies' assumptions about non-labor costs will be taken into account in any future estimate of the burden for this collection.

Other costs mentioned in this comment, such as the cost of customer service time, printing checks, and embossing cards, are costs that the institution would incur regardless of the implementation of the final Guidance. These costs are not associated with an information collection, and, therefore, have not been factored into the NCUA Board's cost estimates.

In addition, the estimates in this comment are based on the assumption that notice should always be provided by mail. However, the final Guidance states that credit unions should deliver member notice in any manner designed to ensure that a member can reasonably be expected to receive it, such as by telephone, mail, or electronically for those members for whom it has a valid e-mail address and who have agreed to receive communications electronically. The NCUA Board assumes that given this flexibility, credit unions may not necessarily choose to mail notices in every case, but may choose less expensive methods of delivery that ensure members will reasonably be expected to receive notice.

Another commenter concerned about the burdens imposed on consumer reporting agencies provided an example of a security breach involving a single company from which identifying information was stolen from about 500,000 military families. Among other things, the company's notice to its customers advised them to contact the nationwide consumer reporting agencies. The commenter stated that the nationwide consumer reporting agencies spent approximately $1.5 million per company, handling approximately 365,000 inquiries from the company's customers.

The final Guidance contains a number of changes that will diminish the costs identified by these commenters. First, the standard for notification in the final Guidance likely will result in fewer notices. In addition, the final Guidance no longer states that all notices should advise members to contact the nationwide consumer reporting agencies. Therefore, the NCUA Board estimates do not factor in the costs to the reporting agencies.

Regulatory Flexibility Act

The Regulatory Flexibility Act (5 U.S.C. 601–612) (RFA) requires an agency to prepare a final regulatory flexibility analysis whenever the agency promulgates a final rule that may have a significant economic impact on a substantial number of small entities. As required by the RFA, the NCUA Board prepared and published an initial regulatory flexibility analysis at the time it issued the proposed rule amending § 748.0 and the proposed guidance in the form of Appendix B. This section contains the Board's final regulatory flexibility analysis.

A. Need for and Objectives of the Rule

As more fully discussed in the preamble to the final rule, section 501 of GLBA requires NCUA to publish standards for federally insured credit unions relating to their security programs to: (1) Insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer. The final rule establishes that federally insured credit unions must include a response program as an element of their security program, and the final Guidance describes the features that a response program should contain to ensure that breaches of security do not

result in harm or inconvenience to members.

B. Summary of Issues Raised by Public Comment

The NCUA Board received no public comment specifically responding to the initial regulatory flexibility analysis contained in the proposed rule. All federally insured credit unions, regardless of size, are subject to GLBA and the rule. The Board believes the changes in the final Guidance, including the standard for determining when to provide notice to members and the increased emphasis on risk-based factors, make the final Guidance easier for smaller credit unions to use. For example, smaller credit unions that offer a relatively less sophisticated array of products and services present a relatively lower level of risk of security breach affecting member information. For these credit unions, the final Guidance contemplates a relatively less comprehensive response program, commensurate with the relatively lower level of risk. Another example of flexibility benefiting smaller institutions relates to service providers. The final Guidance contemplates that, where a service provider maintains member information, a credit union may delegate authority to that service provider to notify members affected by a security breach on its behalf. The Board believes this flexibility is of particular benefit to smaller credit unions, which typically use service providers and may not have the resources to provide timely and effective notice themselves.

C. Consideration of Alternatives

All federally insured credit unions are already required by GLBA and existing regulation to develop and implement a security program. Development of an effective program involves: Assessing risks to member information; establishing policies, procedures, and training to control risks; testing the program's effectiveness; and managing and monitoring service providers. The NCUA Board believes establishing an information security program is a sound business practice for all credit unions and is already addressed by existing supervisory procedures. The final rule requires that security programs include a provision for appropriate responses to incidents involving a breach of information integrity. Consistent with the position taken by the Banking Agencies, the Board views this as a fundamental element of any information security program. Members of smaller credit unions are entitled to expect their personal financial information will be protected and that their credit union will respond appropriately and effectively to any breach of security. Ultimately, there is no alternative to requiring that all credit unions include an effective response program as an element of their security programs.

Nevertheless, the Board specifically solicited comment in the proposed rule on any significant alternatives, consistent with GLBA, that would minimize the impact on small credit unions. As more fully discussed in the preamble to the final rule and in the preceding section of this analysis, the final Guidance provides substantial flexibility so that any credit union, regardless of size, may adopt an information security program tailored to its individual needs.

Executive Order 13132

Executive Order 13132 encourages independent regulatory agencies to consider the impact of their actions on state and local interests. In adherence to fundamental federalism principles, NCUA, an independent regulatory agency as defined in 44 U.S.C. 3502(5), voluntarily complies with the executive order. The final rule would not have substantial direct effects on the states, on the connection between the national government and the states, or on the distribution of power and responsibilities among the various levels of government. NCUA has determined that this final rule does not constitute a policy that has federalism implications for purposes of the executive order.

The Treasury and General Government Appropriations Act, 1999—Assessment of Federal Regulations and Policies on Families

The NCUA has determined that this final rule would not affect family well-being within the meaning of section 654 of the Treasury and General Government Appropriations Act, 1999, Public Law 105–277, 112 Stat. 2681 (1998).

Agency Regulatory Goal

NCUA's goal is to promulgate clear and understandable regulations that impose minimal regulatory burden. We invite your comments on whether the final rule is understandable and minimally intrusive.

List of Subjects in 12 CFR Part 748

Credit unions, Crime, Currency, Reporting and recordkeeping requirements and Security measures.

By the National Credit Union Administration Board on April 14, 2005.

Mary F. Rupp,

Secretary of the Board.

■ For reasons set forth in the preamble, the NCUA Board proposes to amend 12 CFR 748 as follows:

PART 748—SECURITY PROGRAM, REPORT OF CRIME AND CATASTROPHIC ACT AND BANK SECRECY ACT COMPLIANCE

■ 1.The authority citation for part 748 reads as follows:

Authority: 12 U.S.C. 1766(a), 1786(Q); 15 U.S.C. 6801 and 6805(b); 31 U.S.C. 5311 and 5318.

■ 2.In § 748.0 revise paragraph (b) to read as follows:

§ 748.0 Security program.

* * * * * *

(b) The security program will be designed to:

(1) Protect each credit union office from robberies, burglaries, larcenies, and embezzlement;

(2) Ensure the security and confidentiality of member records, protect against the anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to a member;

(3) Respond to incidents of unauthorized access to or use of member information that could result in substantial harm or serious inconvenience to a member;

(4) Assist in the identification of persons who commit or attempt such actions and crimes, and

(5) Prevent destruction of vital records, as defined in 12 CFR part 749.

■ 3. Add Appendix B to read as follows:

Appendix B to Part 748—Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice

I. Background

This Guidance in the form of Appendix B to NCUA's Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance regulation,[29] interprets section 501(b) of the Gramm-Leach-Bliley Act (''GLBA'') and describes response programs, including member notification procedures, that a federally insured credit union should develop and implement to address unauthorized access to or use of member information that could result in substantial harm or inconvenience to a member. The scope of, and definitions of terms used in,

[29] 12 CFR Part 748.

this Guidance are identical to those of Appendix A to Part 748 (Appendix A). For example, the term ''member information'' is the same term used in Appendix A, and means any record containing nonpublic personal information about a member, whether in paper, electronic, or other form, maintained by or on behalf of the credit union.

A. Security Guidelines

Section 501(b) of the GLBA required the NCUA to establish appropriate standards for credit unions subject to its jurisdiction that include administrative, technical, and physical safeguards to protect the security and confidentiality of member information. Accordingly, the NCUA amended Part 748 of its rules to require credit unions to develop appropriate security programs, and issued Appendix A, reflecting its expectation that every federally insured credit union would develop an information security program designed to:

1. Ensure the security and confidentiality of member information;

2. Protect against any anticipated threats or hazards to the security or integrity of such information; and

3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any member.

B. Risk Assessment and Controls

1. Appendix A directs every credit union to assess the following risks, among others, when developing its information security program:

a. Reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of member information or member information systems;

b. The likelihood and potential damage of threats, taking into consideration the sensitivity of member information; and

c. The sufficiency of policies, procedures, member information systems, and other arrangements in place to control risks.[30]

2. Following the assessment of these risks, Appendix A directs a credit union to design a program to address the identified risks. The particular security measures a credit union should adopt will depend upon the risks presented by the complexity and scope of its business. At a minimum, the credit union should consider the specific security measures enumerated in Appendix A,[31] and adopt those that are appropriate for the credit union, including:

a. Access controls on member information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing member information to unauthorized individuals who may seek to obtain this information through fraudulent means;

b. Background checks for employees with responsibilities for access to member information; and

c. Response programs that specify actions to be taken when the credit union suspects or detects that unauthorized individuals have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies.[32]

C. Service Providers

Appendix A advises every credit union to require its service providers by contract to implement appropriate measures designed to protect against unauthorized access to or use of member information that could result in substantial harm or inconvenience to any member.[33]

II. Response Program

i. Millions of Americans, throughout the country, have been victims of identity theft.[34] Identity thieves misuse personal information they obtain from a number of sources, including credit unions, to perpetrate identity theft. Therefore, credit unions should take preventative measures to safeguard member information against such attempts to gain unauthorized access to the information. For example, credit unions should place access controls on member information systems and conduct background checks for employees who are authorized to access member information.[35] However, every credit union should also develop and implement a risk-based response program to address incidents of unauthorized access to member information in member information systems that occur nonetheless.[36] A response program should be a key part of a credit union's information security program.[37] The program should be appropriate to the size and complexity of the credit union and the nature and scope of its activities.

ii. In addition, each credit union should be able to address incidents of unauthorized access to member information in member information systems maintained by its domestic and foreign service providers. Therefore, consistent with the obligations in this Guidance that relate to these arrangements, and with existing guidance on this topic issued by the NCUA,[38] a credit union's contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to or use of the credit union's member information, including notification of the credit union as soon as possible of any such incident, to enable the institution to expeditiously implement its response program.

A. Components of a Response Program

1. At a minimum, a credit union's response program should contain procedures for the following:

a. Assessing the nature and scope of an incident, and identifying what member information systems and types of member information have been accessed or misused;

b. Notifying the appropriate NCUA Regional Director, and, in the case of state-chartered credit unions, its applicable state supervisory authority, as soon as possible when the credit union becomes aware of an incident involving unauthorized access to or use of sensitive member information as defined below.

c. Consistent with the NCUA's Suspicious Activity Report (''SAR'') regulations,[39] notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;

d. Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of member information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; [40] and

e. Notifying members when warranted.

2. Where an incident of unauthorized access to member information involves member information systems maintained by a credit union's service providers, it is the responsibility of the credit union to notify the credit union's members and regulator. However, a credit union may authorize or contract with its service provider to notify the credit union's members or regulators on its behalf.

III. Member Notice

i. Credit unions have an affirmative duty to protect their members' information against

[30] *See* 12 CFR Part 748, Appendix A, Paragraph III.B.

[31] *See* Appendix A, paragraph III.C.

[32] *See* Appendix A, Paragraph III.C.

[33] *See* Appendix A, Paragraph III.B. and III.D. Further, the NCUA notes that, in addition to contractual obligations to a credit union, a service provider may be required to implement its own comprehensive information security program in accordance with the Safeguards Rule promulgated by the Federal Trade Commission (ldquo;FTC''), 12 CFR Part 314.

[34] The FTC estimates that nearly 10 million Americans discovered they were victims of some form of identify theft in 2002. *See* The Federal Trade Commission, *Identity Theft Survey Report,* (September 2003), available at *http://www.ftc.gov/os/2003/09synovatereport.pdf.*

[35] Credit unions should also conduct background checks of employees to ensure that the credit union does not violate 12 U.S.C. 1785(d), which prohibits a credit union from hiring an individual convicted of certain criminal offenses or who is subject to a prohibition order under 12 U.S.C. 1786(g).

[36] Under 12 CFR Part 748, Appendix A, a credit union's *member information systems* consists of all of the methods used to access, collect, store, use, transmit, protect, or dispose of member information, including the systems maintained by its service providers. *See* 12 CFR Part 748, Appendix A, Paragraph I.C.2.d.

[37] *See* FFIEC Information Technology Examination Handbook, Information Security Booklet, (December, 2002), available at *http://www.ffiec.gov/ffiecinfobase/html—pages/it—01.htm1●infosec,* for additional guidance on preventing, detecting, and responding to intrusions into financial institution computer systems.

[38] *See* FFIEC Information Technology Examination Handbook, Outsourcing Technology Services Booklet, (June 2004), available at *http://www.ffiec.gov/ffiecinfobase/html—pages/it—01.htm1●outscouring* for additional guidance on managing outsourced relationships.

[39] A credit union's obligation to file a SAR is set out in the NCUA's SAR regulations and guidance. *See* 12 CFR Part 748.1(c); NCUA Letter to Credit Unions No. 04–CU–03, Suspiciouis Activity Reports, March 2004; NCUA Regulatory Alert No. 04–RA–01, The Suspicious Activity Report (SAR) Activity Review—Trends, Tips, & Isues, Issue 6, November 2003, February 2004.

[40] *See* FFIEC Information Technology Examination Handbook, Information Security Booklet, (December 2002), pp. 68–74.

unauthorized access or use. Notifying members of a security incident involving the unauthorized access or use of the member's information in accordance with the standard set forth below is a key part of that duty.

ii. Timely notification of members is important to manage a credit union's reputation risk. Effective notice also may reduce a credit union's legal risk, assist in maintaining good member relations, and enable the credit union's members to take steps to protect themselves against the consequences of identity theft. When member notification is warranted, a credit union may not forgo notifying its customers of an incident because the credit union believes that it may be potentially embarrassed or inconvenienced by doing so.

A. Standard for Providing Notice

When a credit union becomes aware of an incident of unauthorized access to sensitive member information, the credit union should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the credit union determines that misuse of its information about a member has occurred or is reasonably possible, it should notify the affected member as soon as possible. Member notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the credit union with a written request for the delay. However, the credit union should notify its members as soon as notification will no longer interfere with the investigation.

1. Sensitive Member Information

Under Part 748.0, a credit union must protect against unauthorized access to or use of member information that could result in substantial harm or inconvenience to any member. Substantial harm or inconvenience is most likely to result from improper access to *sensitive member information* because this type of information is most likely to be misused, as in the commission of identity theft.

For purposes of this Guidance, sensitive member information means a member's name, address, or telephone number, in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the member's account. *Sensitive member information* also includes any combination of components of member information that would allow someone to log onto or access the member's account, such as user name and password or password and account number.

2. Affected Members

If a credit union, based upon its investigation, can determine from its logs or other data precisely which members' information has been improperly accessed, it may limit notification to those members with regard to whom the credit union determines that misuse of their information has occurred or is reasonably possible. However, there may be situations where the credit union determines that a group of files has been accessed improperly, but is unable to identify which specific member's information has been accessed. If the circumstances of the unauthorized access lead the credit union to determine that misuse of the information is reasonably possible, it should notify all members in the group.

B. Content of Member Notice

1. Member notice should be given in a clear and conspicuous manner. The notice should describe the incident in general terms and the type of member information that was the subject of unauthorized access or use. It also should generally describe what the credit union has done to protect the members' information from further unauthorized access. In addition, it should include a telephone number that members can call for further information and assistance.[41] The notice also should remind members of the need to remain vigilant over the next twelve to twenty-four months, and to promptly report incidents of suspected identity theft to the credit union. The notice should include the following additional items, when appropriate:

a. A recommendation that the member review account statements and immediately report any suspicious activity to the credit union;

b. A description of fraud alerts and an explanation of how the member may place a fraud alert in the member's consumer reports to put the member's creditors on notice that the member may be a victim of fraud;

c. A recommendation that the member periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;

d. An explanation of how the member may obtain a credit report free of charge; and

e. Information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft. The notice should encourage the member to report any incidents of identity theft to the FTC, and should provide the FTC's Web site address and toll-free telephone number that members may use to obtain the identity theft guidance and report suspected incidents of identity theft.[42]

2. NCUA encourages credit unions to notify the nationwide consumer reporting agencies prior to sending notices to a large number of members that include contact information for the reporting agencies.

C. Delivery of Member Notice

Member notice should be delivered in any manner designed to ensure that a member can reasonably be expected to receive it. For example, the credit union may choose to contact all members affected by telephone or by mail, or by electronic mail for those members for whom it has a valid e-mail address and who have agreed to receive communications electronically.

[FR Doc. 05–7836 Filed 4–29–05; 8:45 am]

BILLING CODE 7535–01–P

[41] The credit union should, therefore, ensure that it has reasonable policies and procedures in place, including trained personnel, to respond appropriately to member inquiries and requests for assistance.

[42] Currently, the FTC Web site for the ID Theft brochure and the FTC Hotline phone number are *http://www.ftc.gov/idtheft* and 1–877–IDTHEFT. The credit union may also refer members to any materials developed pursuant to section 15(1)(b) of the FACT Act (educational materials developed by the FTC to teach the public how to prevent identity theft).

DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

12 CFR Part 41

[Docket No. 05–10]

RIN 1557–AC85

FEDERAL RESERVE SYSTEM

12 CFR Parts 222 and 232

[Regulation V and FF; Docket No. R–1188]

FEDERAL DEPOSIT INSURANCE CORPORATION

12 CFR Part 334

RIN 3064–AC81

DEPARTMENT OF THE TREASURY

Office of Thrift Supervision

12 CFR Part 571

[No. 2005–16]

RIN 1550–AB88

NATIONAL CREDIT UNION ADMINISTRATION

12 CFR Part 717

Fair Credit Reporting Medical Information Regulations

AGENCIES: Office of the Comptroller of the Currency, Treasury (OCC); Board of Governors of the Federal Reserve System (Board); Federal Deposit Insurance Corporation (FDIC); Office of Thrift Supervision, Treasury (OTS); National Credit Union Administration (NCUA).

ACTION: Interim final rules; request for public comments.

SUMMARY: The OCC, Board, FDIC, OTS, and NCUA (Agencies) are publishing interim final rules to implement section 411 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). The interim final rules create exceptions to the statute's general prohibition on creditors obtaining or using medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit for all creditors. The exceptions permit creditors to obtain or use medical information in connection with credit eligibility determinations where necessary and appropriate for legitimate purposes, consistent with the Congressional intent to restrict the use of medical information for inappropriate purposes. The interim final rules also create limited exceptions to permit affiliates to share medical information with each other without becoming consumer reporting agencies.

DATES: This interim final rule is effective March 7, 2006. Comments must be received by July 11, 2005.

ADDRESSES: Comments should be directed to:

OCC: You should include OCC and Docket Number 05–10 in your comment. You may submit comments by any of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *OCC Web Site: http://www.occ.treas.gov.* Click on ''Contact the OCC,'' scroll down and click on ''Comments on proposed regulations.''
- *E-mail Address: regs.comments@occ.treas.gov.*
- *Fax:* (202) 874–4448.
- *Mail:* Office of the Comptroller of the Currency, 250 E Street, SW., Mail Stop 1–5, Washington, DC 20219.
- *Hand Delivery/Courier:* 250 E Street, SW., Attn: Public Information Room, Mail Stop 1–5, Washington, DC 20219.

Instructions: All submissions received must include the agency name (OCC) and docket number or Regulatory Information Number (RIN) for this rulemaking. In general, OCC will enter all comments received into the docket without change, including any business or personal information that you provide. You may review comments and other related materials by any of the following methods:

- *Viewing Comments Personally:* You may personally inspect and photocopy comments at the OCC's Public Information Room, 250 E Street, SW., Washington, DC. You can make an appointment to inspect comments by calling (202) 874–5043.
- *Viewing Comments Electronically:* You may request e-mail or CD–ROM copies of comments that the OCC has received by contacting the OCC's Public Information Room at *regs.comments@occ.treas.gov.*
- *Docket:* You may also request available background documents and project summaries using the methods described above.

Board: You may submit comments, identified by Docket No. R–1188, by any of the following methods:

- *Agency Web Site: http://www.federalreserve.gov.* Follow the instructions for submitting comments at *http://www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm.*
- *Federal eRulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *E-mail: regs.comments@federalreserve.gov.* Include docket number in the subject line of the message.
- *Fax:* 202/452–3819 or 202/452–3102.
- *Mail:* Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System, 20th Street and Constitution Avenue, NW., Washington, DC 20551.

All public comments are available from the Board's Web site at *http://www.federalreserve.gov/generalinfo/foia/ProposedRegs.cfm* as submitted, except as necessary for technical reasons. Accordingly, your comments will not be edited to remove any identifying or contact information. Public comments may also be viewed electronically or in paper in Room MP–500 of the Board's Martin Building (20th and C Streets, NW.) between 9 a.m. and 5 p.m. on weekdays.

FDIC: You may submit comments, identified by RIN number by any of the following methods:

- *Agency Web Site: http://www.fdic.gov/regulations/laws/federal/propose.html.* Follow instructions for submitting comments on the Agency Web Site.
- *E-Mail: Comments@FDIC.gov.* Include the RIN number in the subject line of the message.
- *Mail:* Robert E. Feldman, Executive Secretary, Attention: Comments, Federal Deposit Insurance Corporation, 550 17th Street, NW., Washington, DC 20429.
- *Hand Delivery/Courier:* Guard station at the rear of the 550 17th Street Building (located on F Street) on business days between 7 a.m. and 5 p.m.
- *Instructions:* All submissions received must include the agency name and RIN for this rulemaking. All comments received will be posted without change to *http://www.fdic.gov/regulations/laws/federal/propose.html* including any personal information provided.

OTS: You may submit comments, identified by number 2005–16, by any of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *E-mail Address: regs.comments@ots.treas.gov.* Please include number 2005–16 in the subject line of the message and include your name and telephone number in the message.
- *Fax:* (202) 906–6518.
- *Mail:* Regulation Comments, Chief Counsel's Office, Office of Thrift

Supervision, 1700 G Street, NW., Washington, DC 20552, Attention: No. 2005–16.

• *Hand Delivery/Courier:* Guard's Desk, East Lobby Entrance, 1700 G Street, NW., from 9 a.m. to 4 p.m. on business days, Attention: Regulation Comments, Chief Counsel's Office, Attention: No. 2005–16.

Instructions: All submissions received must include the agency name and docket number or Regulatory Information Number (RIN) for this rulemaking. All comments received will be posted without change to the OTS Internet Site at *http://www.ots.treas.gov/pagehtml.cfm?catNumber=67&an=1,* including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to *http://www.ots.treas.gov/pagehtml.cfm?catNumber=67&an=1.* In addition, you may inspect comments at the Public Reading Room, 1700 G Street, NW., by appointment. To make an appointment for access, call (202) 906–5922, send an e-mail to *public.info@ots.treas.gov,* or send a facsimile transmission to (202) 906–7755. (Prior notice identifying the materials you will be requesting will assist us in serving you.) We schedule appointments on business days between 10 a.m. and 4 p.m. In most cases, appointments will be available the next business day following the date we receive a request.

NCUA: You may submit comments by any of the following methods (Please send comments by one method only):

• *Federal eRulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.

• *NCUA Web Site: http://www.ncua.gov/RegulationsOpinionsLaws/proposed__regs/proposed__regs.html.* Follow the instructions for submitting comments.

• *E-mail:* Address to *regcomments@ncua.gov.* Include ''[Your name] Comments on Interim Final Rule Part 717, Fair Credit Reporting—Medical Information'' in the e-mail subject line.

• *Fax:* (703) 518–6319. Use the subject line described above for e-mail.

• *Mail:* Address to Mary Rupp, Secretary of the Board, National Credit Union Administration, 1775 Duke Street, Alexandria, Virginia 22314–3428.

• *Hand Delivery/Courier:* Address to Mary Rupp, Secretary of the Board, National Credit Union Administration. Deliver to guard station in the lobby of 1775 Duke Street, Alexandria, Virginia 22314–3428, on business days between 8 a.m. and 5 p.m.

All public comments are available on the agency's Web site at *http://www.ncua.gov/RegulationsOpinionsLaws/comments* as submitted, except as may not be possible for technical reasons. Public comments will not be edited to remove any identifying or contact information. Paper copies of comments may be inspected in NCUA's law library, at 1775 Duke Street, Alexandria, Virginia 22314, by appointment weekdays between 9 a.m. and 3 p.m. To make an appointment, call (703) 518–6546 or send an e-mail to *OGCMail@ncua.gov.*

FOR FURTHER INFORMATION CONTACT:

OCC: Amy Friend, Assistant Chief Counsel, (202) 874–5200; Michael Bylsma, Director, or Stephen Van Meter, Assistant Director, Community and Consumer Law, (202) 874–5750; Patrick T. Tierney, Senior Attorney, Legislative and Regulatory Activities Division, (202) 874–5090; or Carol Turner, Compliance Specialist, Compliance Department, (202) 874–4858, Office of the Comptroller of the Currency, 250 E Street, SW., Washington, DC 20219.

Board: David A. Stein, Counsel; Minh-Duc T. Le, Ky Tran-Trong, or Krista P. DeLargy, Senior Attorneys, Division of Consumer and Community Affairs, (202) 452–3667 or (202) 452–2412; or Andrew Miller, Counsel, Legal Division, (202) 452–3428, Board of Governors of the Federal Reserve System, 20th and C Streets, NW., Washington, DC 20551.

FDIC: Richard M. Schwartz, Counsel, Legal Division, (202) 898–7424; David Lafleur, Policy Analyst, (202) 898–6569, or Patricia Cashman, Senior Policy Analyst, Division of Supervision and Consumer Protection, (202) 898–6534, Federal Deposit Insurance Corporation, 550 17th Street, NW., Washington, DC 20429.

OTS: Elizabeth Baltierra, Program Analyst (Compliance), Compliance Policy, (202) 906–6540; Richard Bennett, Counsel, (202) 906–7409; Judith A. McCormick, Director, Consumer Protection and Specialty Programs, (202) 906–5636, Office of Thrift Supervision, 1700 G Street, NW., Washington, DC 20552.

NCUA: Regina M. Metz, Staff Attorney, Office of General Counsel, (703) 518–6540, National Credit Union Administration, 1775 Duke Street, Alexandria, VA 22314–3428.

SUPPLEMENTARY INFORMATION:

I. Background

The FACT Act became law on December 4, 2003. Pub. L. 108–159, 117 Stat. 1952. In general, the FACT Act amends the Fair Credit Reporting Act (FCRA or Act) to enhance the ability of consumers to combat identity theft, increase the accuracy of consumer reports, and allow consumers to exercise greater control regarding the type and amount of marketing solicitations they receive. Section 411 of the FACT Act generally limits the ability of creditors to obtain or use medical information in connection with credit eligibility determinations, consumer reporting agencies to disclose medical information, and all persons to share medical information and other medical-related information with affiliates.

Section 411(a) of the FACT Act adds a new section 604(g)(1) to the FCRA to restrict the circumstances under which consumer reporting agencies may furnish consumer reports that contain medical information about consumers. Under section 604(g)(1), a consumer reporting agency may not furnish a consumer report that contains medical information about a consumer unless:

(1) The report is furnished in connection with an insurance transaction, and the consumer affirmatively consents to the furnishing of the report;

(2) The report is furnished for employment purposes or in connection with a credit transaction, the information to be furnished is relevant to process or effect the employment or credit transaction, and the consumer provides specific written consent for the furnishing of the report that describes in clear and conspicuous language the use for which the information will be furnished; or

(3) The information to be furnished pertains solely to transactions, accounts, or balances relating to debts arising from the receipt of medical services, products, or devices, where such information, other than account status or amounts, is restricted or reported using codes that do not identify, or do not provide information sufficient to infer, the specific provider or the nature of such services, products, or devices.

Section 411(c) of the FACT Act revises the definition of ''medical information'' in section 603(i) to mean information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to the past, present, or future physical, mental, or behavioral health or condition of an individual, the provision of health care to an individual, or the payment for the provision of health care to an individual. The term ''medical

information'' does not include the age or gender of a consumer, demographic information about the consumer, including a consumer's residence address or e-mail address, or any other information about a consumer that does not relate to the physical, mental, or behavioral health or condition of a consumer, including the existence or value of any insurance policy.

Section 411(a) also amends the FCRA by adding new section 604(g)(2) to prohibit creditors from obtaining or using medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit. Section 604(g)(2) contains two independent prohibitions—a prohibition on obtaining medical information and a prohibition on using medical information. The statute contains no prohibition, however, on creditors obtaining or using medical information other than in connection with a determination of the consumer's eligibility, or continued eligibility, for credit. For example, section 604(g)(2) does not prohibit a creditor from obtaining medical information in connection with employment purposes. Nevertheless, a creditor that obtains medical information in connection with employment purposes may not subsequently use that information in connection with any determination of the consumer's eligibility, or continued eligibility, for credit. Section 604(g)(5)(A) requires the Agencies to prescribe regulations that permit transactions that are determined to be necessary and appropriate to protect legitimate operational, transactional, risk, consumer, and other needs (including administrative verification purposes), consistent with Congressional intent to restrict the use of medical information for inappropriate purposes.

Section 411(b) of the FACT Act adds a new section 603(d)(3) to the FCRA to restrict the sharing of medically related information with affiliates if that information meets the definition of ''consumer report'' in section 603(d)(1) of the FCRA. Specifically, section 603(d)(3) provides that the standard exclusions from the definition of ''consumer report'' contained in section 603(d)(2)—such as sharing transaction or experience information among affiliates or sharing other information among affiliates after notice and an opportunity to opt-out—do not apply if medically related information is disclosed to an affiliate. Medically related information includes medical information, as described above, as well as an individualized list or description based on payment transactions for medical products or services, and an aggregate list of identified consumers based on payment transactions for medical products or services.

Section 604(g)(3), however, provides several exceptions that allow institutions to share medically related information with affiliates in accordance with the standard exclusions that apply to the sharing of non-medically related information. These exceptions provide that an institution may share medically related information with an affiliate without having the communication categorically treated as a consumer report if the information is disclosed to an affiliate:

(1) In connection with the business of insurance or annuities (including the activities described in section 18B of the model Privacy of Consumer Financial and Health Information Regulation issued by the National Association of Insurance Commissioners, as in effect on January 1, 2003);

(2) For any purpose permitted without authorization under the Standards for Individually Identifiable Health Information promulgated by the Department of Health and Human Services (HHS) pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA);

(3) For any purpose referred to under section 1179 of HIPAA;

(4) For any purpose described in section 502(e) of the Gramm-Leach-Bliley Act; or

(5) As otherwise determined to be necessary and appropriate, by regulation or order, by the Federal Trade Commission (FTC), the Agencies, or an applicable State insurance authority.

Section 604(g)(4), as added by section 411(a)(4) of the FACT Act, also provides that any person that receives medical information from an affiliate pursuant to an exception in section 604(g)(3) or from a consumer reporting agency under section 604(g)(1) must not disclose such information to any other person, except as necessary to carry out the purpose for which the information was initially disclosed, or as otherwise permitted by statute, regulation, or order.

II. Overview of Comments Received

On April 28, 2004, the Agencies published a notice of proposed rulemaking in the **Federal Register** (69 FR 23380) to implement the provisions of section 411 of the FACT Act. The Agencies proposed to create exceptions to the general prohibition against creditors obtaining or using medical information in connection with credit eligibility determinations, as required by section 604(g)(5)(A), to permit transactions necessary and appropriate to protect legitimate operational, transactional, risk, consumer, and other needs (including administrative verification purposes), consistent with the intent of Congress to restrict the use of medical information for inappropriate purposes. In addition, the Agencies proposed to create additional exceptions to the special restrictions in section 603(d)(3) on sharing medically related information with affiliates, as permitted by section 604(g)(3)(C).

Each of the Agencies received up to 40 comment letters in response to the proposal, although many commenters sent copies of the same letter to more than one Agency. Comments were received from a variety of industry commenters, including banks, thrifts, credit unions, credit card companies, mortgage lenders and other non-bank creditors, and industry trade associations. Comments were also received from insurance companies and insurance industry trade associations. Other comments were received from consumer and community groups, privacy advocates, and health care associations. A comment letter was received from two Members of Congress, and another comment letter was received from the Federal Trade Commission.

Most commenters supported the proposed rule. Commenters offered a number of suggested changes, with the most common suggestions including: broadening the scope of coverage to apply to all creditors; broadening the scope of coverage to apply to an individual's credit eligibility made in connection with business credit; clarifying the definition of ''medical information'; implementing the statute by relying primarily on interpretations of the statute rather than exceptions; addressing debt cancellation contracts, debt suspension agreements, and credit insurance products through an exception; and revising the language and scope of various exceptions to the general prohibition on obtaining and using medical information.

The Agencies have modified the proposed rule in light of the comments received. These comments, and the Agencies' responses to the comments, are discussed in the following section-by-section analysis. As discussed below, the Agencies are adopting these rules as interim final rules so that interested parties may comment on the expanded scope of the exceptions for obtaining and using medical information in connection with credit eligibility determinations.

III. Section-by-Section Analysis

Section __.2 Examples

Section __.2 of the proposal discussed the scope and effect of the examples included in the proposed rule. Commenters supported the provision regarding the scope and effect of examples. Section __.2 is therefore adopted as proposed.

Section __.3 Definitions

Section __.3 of the proposal contained definitions for the terms ''affiliate'' (as well as the related terms ''company'' and ''control''), ''consumer,'' ''medical information,'' and ''you.'' The proposed definition of ''you'' has not been included in the interim final rule as unnecessary.[1]

Affiliate

Several FCRA provisions apply to information sharing with persons ''related by common ownership or affiliated by corporate control,'' ''related by common ownership or affiliated by common corporate control,'' or ''affiliated by common ownership or common corporate control.'' *E.g.*, FCRA, sections 603(d)(2), 615(b)(2), and 624(b)(2). Each of these provisions was enacted as part of the 1996 amendments to the FCRA. Similarly, section 2 of the FACT Act defines the term ''affiliate'' to mean persons that are related by common ownership or affiliated by corporate control.

Under the proposal, the Agencies proposed to define ''affiliate'' to mean any company that controls, is controlled by, or is under common control with another company, which is identical to the definition of ''affiliate'' in section 509 of the GLB Act and the GLB Act privacy regulations. The Agencies received very few comments on the definition of ''affiliate'' and none that suggested changes to the definition.

In the interim final rules, the Agencies have revised the definition of ''affiliate'' to track more closely the definition contained in section 2 of the FACT Act. Section __.3(b) of the interim final rules defines ''affiliate'' to mean any company that is related by common ownership or common corporate control with another company.[2]

The Agencies believe there is no substantive difference between the FACT Act definition of ''affiliate'' and the definition of ''affiliate'' in section 509 of the GLB Act. The Agencies are not aware of any circumstances in which two entities would be affiliates for purposes of the FCRA but not for purposes of the GLB Act privacy rules, or vice versa. Furthermore, even though affiliated entities have had to comply with different formulations of the ''affiliate'' definition under the FCRA and the GLB Act since 1999, the Agencies are not aware of any compliance difficulties or disputes resulting from the two statutes using somewhat different wording to describe what constitutes an affiliate.

Under the GLB Act privacy rules, the definition of ''control'' determines whether two or more entities meet the definition of ''affiliate.'' [3] The Agencies included the same definition of ''control'' in the proposal. The Agencies received no comments on the proposed definition of ''control.'' Accordingly, the Agencies interpret the phrase ''related by common ownership or common corporate control'' as used in the FACT Act to have the same meaning as ''control'' in the GLB Act privacy rules. For example, if an individual owns 25 percent of two companies, the companies would be affiliates under both the GLB Act and FCRA definitions. However, the individual would not be considered an affiliate of the companies because the definition of ''affiliate'' is limited to companies.

For purposes of clarity, the Agencies are revising the defined term from ''control'' (as in the proposal) to ''common ownership or common corporate control'' in order to track more closely the terminology used in the FACT Act.[4] In addition, the Agencies believe that certain types of persons, for example, governments or governmental agencies or individuals are not subject to control, as that term is defined in the interim final rules, for purposes of defining an affiliate.

The proposal also included a definition of ''company,'' which was defined to include any corporation, limited liability company, business trust, general or limited partnership, association, or similar organization. Omitted from the definition of ''company'' are some entities that are ''persons'' under the FCRA, including estates, cooperatives, and governments or governmental subdivisions or agencies, as well as individuals. The Agencies received no comments on the proposed definition of ''company,'' which is adopted as proposed.

The interim final rule includes a definition of ''person'' to reflect that the definition of ''affiliate'' now refers to a ''person'' rather than to a ''company.'' The definition of ''person'' tracks the statutory definition and means any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity.

Medical Information

Under the proposed rule, paragraph (k) defined the term ''medical information'' to mean information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to (1) the past, present, or future physical, mental, or behavioral health or condition of an individual; (2) the provision of health care to an individual; or (3) the payment for the provision of health care to an individual. Proposed paragraph (k) also made clear that the term ''medical information'' did not include the age or gender of a consumer, demographic information about the consumer, including a consumer's residence address or e-mail address, or any other information about a consumer that does not relate to the physical, mental, or behavioral health or condition of a consumer, including the existence or value of any insurance policy. The definition in the proposal tracked the statutory definition of ''medical information.''

The Agencies requested comment on whether coded information furnished by a consumer reporting agency in accordance with section 604(g)(1)(C) of the FCRA should be deemed to fall outside the definition of ''medical information.'' Industry commenters generally believed that coded information should be excluded from the definition of ''medical information'' because Congress, by requiring coding by consumer reporting agencies, determined the appropriate protection for this information. Privacy advocates, consumer and community groups, and health care associations urged the Agencies not to exclude coded information from the definition of ''medical information'' because they believed it would be an inappropriate narrowing of the statutory definition and would effectively remove such information from the anti-discrimination protections of proposed § __.30(c) by allowing creditors to treat medical debts, if coded, differently than non-medical debts. Based on the

[1] The OTS previously added a definition of ''you'' to § 571.3(o) in connection with its disposal rule. *See* 69 FR 77610, 77621 (Dec. 28, 2004). That definition remains in the OTS's rule.

[2] For purposes of the regulation, an ''affiliate'' includes an operating subsidiary of a bank or savings association, and a credit union service organization that is controlled by a Federal credit union.

[3] *See* 12 CFR 40.3(g), 216.3(g), 332.3(g), 573.3(g), and 716.3(g).

[4] For purposes of the regulation, NCUA presumes that a Federal credit union has a controlling influence over the management or policies of a credit union service organization if it is 67 percent owned by credit unions.

comments received and an analysis of the terms and structure of the FACT Act, the Agencies have determined to treat coded information as ''medical information'' for purposes of the Agencies'' rules. The statutory definition of ''medical information'' is quite broad. In addition, the wording of section 604(g)(1) indicates that ''medical information about a consumer'' includes both coded and uncoded information from a consumer report. How creditors may obtain and use this information is discussed below.

A number of commenters asked the Agencies to clarify that ''medical information'' must relate or pertain to a specific consumer. Commenters requested this clarification to ensure that creditors can continue to use databases containing aggregate, non-personally identifiable information about consumers to analyze consumer behavior patterns without violating the restrictions on obtaining or using medical information. The FTC recommended that the Agencies clarify that information about collateral is not ''medical information'' because information about collateral does not pertain to an individual.

The Agencies believe that the statutory definition of ''medical information'' applies only to information that is associated with a specific consumer because such information must relate to the condition ''of an individual'' or the provision of health care or payment for the provision of health care ''to an individual.'' In the interim final rule, the Agencies have clarified that the term ''medical information'' does not include information that does not identify a specific consumer. Section __.3(k)(2)(iv) contains this clarification. The interim final rule does not categorically exclude information about collateral from the definition of medical information because the relationship between information about collateral and medical information about an individual may depend upon the facts and circumstances.

One commenter asked the Agencies to clarify that information about the death of an individual is not medical information. The Agencies believe that the fact that a consumer is deceased generally is not ''medical information.'' However, certain information associated with the death of a consumer, such as information about the medical condition that resulted in the consumer's death, may be medical information.

Creditors are reminded that other laws, such as the Americans with Disabilities Act, the Fair Housing Act (FHA), the GLB Act, the Health Insurance Portability and Accountability Act (HIPAA), and other parts of the FCRA, may limit or regulate the use, collection, and sharing of consumer information, including medical information. These and other laws, such as the Equal Credit Opportunity Act (ECOA), also may prohibit creditors from using certain information that is excluded from the restrictions on obtaining or using medical information, such as age or gender information, in determining eligibility for credit or for other purposes. The exceptions created by this rule do not override or modify, or in any way limit the responsibility of creditors to comply with all applicable Federal and state fair lending laws. The OTS reminds creditors subject to its rules that they must comply with the requirements of the OTS's anti-discrimination rules when seeking to obtain and use medical information in reliance on the exceptions in this rule.[5]

Section __.30 Obtaining or Using Medical Information in Connection With a Determination of Eligibility for Credit

Section 411(a) of the FACT Act adds a new section 604(g)(2) to the FCRA, which contains a broad new limitation on the ability of creditors to either obtain or use medical information in connection with credit eligibility determinations.

A. Scope of Rules on Obtaining or Using Medical Information

Section 604(g)(2) (as added by section 411 of the FACT Act) prohibits any ''creditor'' from obtaining or using ''medical information'' in connection with any determination of the consumer's eligibility, or continued eligibility, for credit.[6] The definition of ''medical information'' adopted in the FACT Act broadly includes information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or a consumer that relates to the past, present, or future physical, mental, or behavioral health or condition of an individual, the provision of health care to an individual, or the payment for the provision of health care to an individual.[7] The definition encompasses important financial information about consumers that is typically used in the credit underwriting process, such as information about the payment history and status of medical debts and the amount of a consumer's disability income.

Section 111 of the FACT Act added a definition of ''creditor'' to the FCRA that is also very broad and includes any person who regularly extends, renews, or continues credit, any person who regularly arranges for the extension, renewal, or continuation of credit, or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.[8] A ''creditor'' includes depository institutions as well as entities that are neither depository institutions nor affiliates of depository institutions, such as independent finance companies, loan brokers, health care providers, and automobile dealers. Accordingly, section 604(g)(2) prohibits all creditors from obtaining or using key financial information that is also medical information in the credit underwriting process.

Section 604(g) does not contain any specific statutory exception to this broad prohibition. Instead, section 604(g)(5) directs the Agencies to prescribe regulations to permit ''transactions'' in which creditors obtain or use medical information that are ''necessary and appropriate to protect legitimate operational, transactional, risk, consumer, and other needs consistent with the intent of paragraph (2) to restrict the use of medical information for inappropriate purposes.'' [9] Section 604(g)(5) does not by its terms limit the scope of the creditors that may rely on exceptions granted by the Agencies.

Proposed § __.1(b)(2) identified the persons to which the rules relating to obtaining and using medical information in proposed §§ __.30(a)–(d) applied. As proposed, each Agency's rule and the exceptions created by those rules applied to creditors subject to the regulatory jurisdiction of the respective Agency. The most significant issue raised by commenters in connection with the proposal related to the classes of creditors to which the exceptions to the statutory prohibition in section 604(g)(2) would apply. Many commenters strongly urged the Agencies to make clear that the regulatory exceptions apply to *all* creditors that are subject to the statutory prohibition on

[5] The OTS's anti-discrimination regulations are found at 12 CFR part 528.

[6] 15 U.S.C. 1681b(g)(2).

[7] *Id.* at § 1681a(i). ''Medical information'' does not include the age or gender of a consumer, demographic information about the consumer, including a consumer's residence address or e-mail address, or any other information about a consumer that does not relate to the physical, mental, or behavioral health or condition of a consumer, including the existence or value of any insurance policy. *Id.*

[8] The meaning of ''creditor'' in the FCRA has the same meaning as in the Equal Credit Opportunity Act (''ECOA''). *Id.* at §§ 1681a(r)(5) and 1691a(e).

[9] *Id.* at § 1681b(g)(5)(A).

obtaining or using medical information, not just bank and thrift creditors and their affiliates and Federal credit unions. Many financial institution creditors indicated that, if the exceptions failed to apply to all creditors, the lending activities of financial institutions would be adversely affected because financial institutions often originate loans through, or purchase loans from, persons that are creditors for purposes of the FCRA but are not financial institutions. In particular, commenters noted that arrangers of credit (which are creditors for purposes of the FCRA) may include doctors and other health care providers that inform consumers of medical financing options and act as a liaison between the consumer and the creditor.

Finally, commenters argued that, without clarification that the classes of creditors that could rely on the Agencies' regulatory exceptions were the same as the classes of creditors subject to the statutory prohibition, a significant number of creditors unaffiliated with banks, thrifts, or Federal credit unions would be in doubt about their ability to obtain and use excepted medical information in the same way and to the same extent as the Agencies' rules allow creditors that are banks, thrifts, Federal credit unions, or affiliates of those institutions to obtain and use the identical information. This result could reduce the availability of credit generally because of the breadth of the statute's definition of medical information. Two Members of Congress who sponsored section 411 of the FACT Act, submitted a comment letter supporting this view and indicating that it was their intention that the exceptions would apply to non-bank finance companies, state-chartered credit unions, and doctors, medical suppliers, and other medical professionals.

The prohibition on creditors obtaining or using medical information in connection with credit eligibility determinations in section 604(g)(2) applies to all creditors. As noted above, section 605(g)(5) does not, by its terms, limit the creditors that may rely on the exceptions granted by the Agencies. Moreover, that section, by its terms, applies to ''transactions'' for which the Agencies determine exceptions are necessary, not to ''creditors'' that the Agencies determine must be protected by the exceptions. Accordingly, the combined scope of the exceptions adopted pursuant to section 604(g)(5) in the interim final rules is as broad as the prohibition to which it applies, and is available to all creditors.

The final action is comprised of six rules. The applicability of the section of each Agency's rule addressing the prohibition on and exceptions for creditors obtaining or using medical information in connection with credit eligibility determinations is set forth in § __.30(a) and covers transactions in which certain enumerated entities participate as creditors. Under § __.30(a)(2), other entities that participate as creditors in transactions in which an enumerated entity also participates as a creditor are also subject to that Agency's rule.

In addition, a separate rule, codified in part 232 of the Board's chapter of the *Code of Federal Regulations* (hereafter ''separate rule''), affords the exceptions to the prohibition against obtaining and using medical information for credit eligibility determinations generally to all creditors, except for creditors that are subject to one of the other Agencies' rules. This combination of rules establishes uniform coverage and exceptions for transactions involving any creditor that is subject to the prohibition on obtaining or using medical information in section 411. The separate rule has been located in the Board's chapter of the Code of Federal Regulations as a matter of convenience because many creditors are accustomed to looking to the Board's regulations implementing other statutes, such as the Truth-in-Lending Act and the Equal Credit Opportunity Act.

The Agencies believe it is important that rules prescribing exceptions to the prohibitions from obtaining or using medical information in connection with credit eligibility determinations be consistent. Thus, in developing the proposed and interim final rules, the Agencies have consulted and coordinated with each other to establish identical rules. The Agencies will consult and coordinate with each other regarding any amendments to the rules for the purpose of assuring, to the extent possible, that the regulations prescribed by each Agency remain consistent and comparable with the regulations prescribed by the other Agencies.

These rules are being adopted on an interim final basis with a delayed effective date. While a number of commenters urged clarification of the scope of the availability of the exceptions, the Agencies are concerned that uncertainty about this matter may have led creditors that believed they could not avail themselves of the exceptions not to comment on the appropriateness and details of the exceptions.

B. General Prohibition on Obtaining or Using Medical Information

Proposed paragraph (a)(1) incorporated the statute's general rule prohibiting creditors from obtaining or using medical information pertaining to a consumer in connection with any determination of a consumer's eligibility, or continued eligibility, for credit, except as provided in the regulations under subpart D. The supplementary information to the proposal noted the consumer's eligibility for credit typically would be determined when an initial decision is made on whether to grant or deny credit to the consumer, but could also include decisions whether to terminate an account or adjust a credit limit following an account review. The Agencies received no comments on this restatement of the statutory prohibition in the proposal. Renumbered paragraph (b)(1) in each Agency's rule and § __.1(b) of the separate rule contain this provision, which is adopted as proposed.

Proposed paragraph (a)(2) clarified the meaning of certain terms used in the statutory prohibition and the proposed rule, including ''eligibility, or continued eligibility, for credit,'' ''credit,'' and ''creditor.'' Commenters had no comments on the definitions of ''credit'' and ''creditor,'' which tracked the FACT Act's definition of those terms. In the interim final rule, renumbered paragraphs (b)(2)(i) and (ii) of each Agency's rule and § __.1(c)(2) and (3) of the separate rule contain the definitions of ''credit'' and ''creditor,'' which are adopted as proposed.

The proposed rule interpreted the phrase ''eligibility, or continued eligibility, for credit'' to mean the consumer's qualification or fitness to receive, or continue to receive, credit, including the terms on which credit is offered, primarily for personal, family, or household purposes. The proposal further clarified that the phrase ''eligibility, or continued eligibility, for credit'' did not include the following: (1) The consumer's qualification or fitness to be offered employment, insurance products, or other non-credit products or services; (2) a determination of whether the provisions of a debt cancellation contract, debt suspension agreement, credit insurance product, or similar forbearance practice or program are triggered; (3) authorizing, processing, or documenting a payment or transaction on behalf of a consumer in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit; or (4) maintaining or servicing a

consumer's account in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit.

Commenters offered a substantial number of suggestions regarding the meaning of ''eligibility, or continued eligibility, for credit.'' Industry commenters supported limiting the term to credit primarily for personal, family, or household purposes consistent with the traditional scope of the FCRA. Privacy advocates, consumer and community groups, and health care associations, on the other hand, objected to the exclusion of business credit from the general prohibition on obtaining or using medical information. These commenters argued that the proposed limitation to consumer credit conflicted with the FCRA definitions of ''credit'' and ''creditor,'' which incorporate the ECOA definitions of those terms. Moreover, these commenters noted that Congress initially used the Truth in Lending Act (TILA) definitions of ''credit'' and ''creditor'' in the draft FACT Act legislation, but subsequently adopted the ECOA definitions of those terms. ECOA applies to business purpose credit, whereas TILA does not.

The Federal banking agencies (OCC, Board, FDIC, and OTS) have previously taken the position that a creditor has a permissible purpose to obtain a consumer report on a consumer in connection with a business credit transaction under section 604(a)(3)(A) of the FCRA if the consumer is or will be personally liable on the loan, such as in the case of a guarantor, co-signer, or, in most instances, an individual proprietor. An informal FTC staff opinion letter concurred with the banking agencies' position. *See* Letter from Joel Winston to Julie L. Williams, J. Virgil Mattingly, William F. Kroener, III, and Carolyn Buck, June 22, 2001. A copy of this letter is available from the FTC's Internet Web site at *http://www.ftc.gov/os/statutes/fcra/tatelbaum2.htm.* To ensure consistency with the prior interpretation, the Agencies are deleting the phrase ''primarily for personal, family, or household purposes'' from the definition of ''eligibility, or continued eligibility, for credit.'' In order for the prohibition in section 604(g)(3) to apply, a creditor must obtain or use medical information about a consumer in connection with a determination of a consumer's eligibility, or continued eligibility, for credit. Accordingly, the general prohibition would apply to business credit if a consumer would be personally liable for repayment of a business loan.

Commenters also pointed to an ambiguity in the proposal: proposed paragraph (a)(2)(i)(A) referred to insurance products while proposed paragraph (a)(2)(i)(B) referred to credit insurance products. To eliminate this ambiguity, the interim final rule has been revised so that renumbered paragraph (b)(2)(iii)(A) of each Agency's rule and section __.1(c)(4)(i) of the separate rule applies to insurance products other than credit insurance products. Additional, non-substantive changes have been made to these paragraphs for clarity.

Commenters made a number of suggestions regarding debt cancellation contracts, debt suspension agreements, and credit insurance products, which were addressed in proposed paragraph (a)(2)(i)(B). Most commenters believed that these contracts, agreements, and products should be addressed through an exception, rather than through an interpretation. In the interim final rule, debt cancellation contracts, debt suspension agreements, and credit insurance products are addressed in two new exceptions, which are discussed below.

Forbearance practices or programs were also addressed in proposed paragraph (a)(2)(i)(B). Most commenters believed that forbearance practices and programs should be addressed through an exception, rather than through an interpretation. In the interim final rule, forbearance practices or programs are addressed in a new exception, which is discussed below.

Under the proposal, the term ''eligibility, or continued eligibility, for credit'' did not include authorizing, processing, or documenting a payment or transaction on behalf of a consumer in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit. The interim final rule retains this interpretation in paragraph (b)(2)(iii)(B). *See also* section __.1(c)(4)(ii) of the separate rule. A few commenters asked the Agencies to clarify that over limit transactions or fees and the use of transaction codes fall within this interpretation. Typically, the routine processing of over limit transactions or the imposition of over limit fees would not involve a determination of the consumer's eligibility, or continued eligibility, for credit. If, however, a creditor has medical information about the consumer and uses that information to determine whether or not to raise the consumer's credit limit, such use must fall within an exception in §§ __.30(d) or (e) of each Agency's rule or §§ __.3 or __.4 of the separate rule to be permissible. Similarly, the use of transaction codes that identify payments to merchants of medical products or services typically would not involve a determination of the consumer's eligibility, or continued eligibility, for credit, unless the creditor uses the medically related codes to make a judgment about whether, and on what terms, to extend credit to the consumer.

Under the proposal, the term ''eligibility, or continued eligibility, for credit'' did not include maintaining or servicing a consumer's account in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit. The interim final rule retains this interpretation in paragraph (b)(2)(iii)(C) of each Agency's rule. *See also* section __.1(c)(4)(iii) of the separate rule.

The FTC recommended adding a number of additional interpretations and deleting or revising references suggesting that the proposed interpretations and rule of construction were not statutory interpretations. In the interim final rule, the Agencies have deleted references that may have suggested that the interpretations are not interpretations of the statute. Most of the additional interpretations recommended by the FTC are addressed elsewhere in this preamble.

One FTC suggestion not addressed elsewhere is the recommendation to interpret the statute to permit doctors and other providers of medical goods and services to extend credit to consumers where the credit is incidental to the provision of medical goods or services. The Agencies agree that providers of medical goods and services ordinarily would obtain medical information pertaining to a consumer in connection with rendering medical care, and not in connection with credit eligibility decisions. Moreover, if a provider did not use that medical information in connection with determining the consumer's eligibility to receive credit, then the provider clearly would not violate the prohibition. For example, a doctor who treats a patient before billing the patient for her services, without considering the patient's payment history or other medical information relating to the patient, would not have obtained and used medical information in connection with an eligibility determination for credit.

As discussed above, the definition of medical information is very broad and includes not only the health or condition of an individual, but information relating to the payment for the provision of health care. *See* section 603(i) of the FCRA (15 U.S.C. 1681a(i)). If a provider uses medical information,

such as a consumer's history of not paying medical bills promptly, in determining whether and on what terms to extend credit to the consumer, then the provider, as a creditor, has used medical information in connection with a credit eligibility determination in contravention of the general prohibition. Thus, the Agencies conclude that an interpretation that excludes incidental credit from the statutory prohibition is not supported by the statute because medical service providers that extend incidental credit may, in some instances, use medical information to determine the consumer's eligibility for such credit.

C. Receiving Unsolicited Medical Information and Coded and Uncoded Information from a Consumer Reporting Agency

Section __.30(b) of the proposal contained a rule of construction regarding the receipt of unsolicited medical information in recognition of the fact that creditors may receive medical information without specifically asking for it. A creditor may receive unsolicited medical information, for example, when a consumer informs the loan officer that she needs a loan to pay for treatment for a particular medical condition, or when a consumer, in response to a general request on a credit application for information about outstanding debts, lists debts owed to hospitals and doctors for medical services. The Agencies proposed a rule of construction to make clear that a creditor would not violate the prohibition on obtaining medical information if the creditor received medical information without specifically asking for or requesting such information and did not use it.

Commenters generally supported the rule of construction for unsolicited medical information. Industry commenters generally favored a rule of construction over an exception.

In addition, the Agencies solicited comment on how to treat information in consumer reports containing information described in section 604(g)(1) of the FCRA. The Agencies solicited comment on three options for allowing creditors to obtain and use coded information contained in a consumer report pursuant to section 604(g)(1)(C). One approach was to interpret ''medical information'' to exclude coded information that may be furnished under section 604(g)(1)(C) of the Act. Another approach was to interpret the prohibition on obtaining or using medical information in section 604(g)(2) as qualified by the provisions in section 604(g)(1) that authorize consumer reporting agencies to furnish consumer reports containing medical information under certain circumstances. A final approach was to require creditors that intend to obtain and use coded medical information in connection with credit eligibility determinations to do so in accordance with the financial information exception in proposed § __.30(c).

Industry commenters generally believed that coded information should be excluded from the definition of ''medical information.'' Privacy advocates, consumer and community groups, and health care associations, on the other hand, maintained that coded information fell within the definition of ''medical information'' and opposed the creation of a separate consumer report exception as in proposed paragraph (d)(1)(iii). These commenters believed that the other proposed exceptions were sufficient to protect legitimate uses of both coded and uncoded medical information obtained from a consumer report. The FTC urged the Agencies to interpret the general prohibition on creditors obtaining and using medical information in section 604(g)(2) as qualified by the provisions in section 604(g)(1) applicable to consumer reporting agencies that furnish consumer reports containing medical information.

As noted above, the Agencies interpret coded information provided pursuant to section 604(g)(1)(C) as meeting the broad statutory definition of ''medical information.'' Under the interim final rules, a creditor that receives medical information from a consumer reporting agency, whether coded or uncoded, without specifically requesting that information does not obtain medical information in violation of the prohibition. Such information, however, may be used only in accordance with the exceptions contained in renumbered paragraphs 30(d) or (e) of each Agency's rule or §§ __.3 or __.4 of the separate rule.

The proposal also included a separate exception for uncoded medical information furnished by a consumer reporting agency in a consumer report pursuant to section 604(g)(1)(B) in proposed paragraph (d)(1)(iii). The proposed exception has been omitted from the interim final rule as unnecessary. Commenters generally did not support this exception. A number of these commenters believed that the other exceptions were sufficient and that no separate exception should be created for consumer reports. The FTC urged the Agencies to treat coded and uncoded medical information furnished by consumer reporting agencies the same by interpreting the general statutory prohibition as inapplicable to such information.

The Agencies believe that the exceptions in renumbered paragraphs (d) and (e) of each Agency's rule and in §§ __.3 and __.4 of the separate rule provide creditors sufficient flexibility with respect to the use of medical information contained in consumer reports. The rule of construction for unsolicited medical information adequately protects creditors that receive coded or uncoded medical information in consumer reports furnished by consumer reporting agencies without specifically requesting medical information. If, however, a creditor specifically requests medical information from a consumer reporting agency in connection with a credit eligibility determination, the creditor must meet one of the exceptions in renumbered paragraphs (d) and (e) of each Agency's rule or §§ __.3 and __.4 of the separate rule in order to obtain and use that information.

Renumbered paragraph (c) of the interim final rule adopts the rule of construction for unsolicited medical information with certain revisions. Section __.2 of the separate rule contains the identical provision. The interim final rule provides that a creditor does not *obtain* medical information in violation of the prohibition if it receives such information from a consumer, a consumer reporting agency, or any other person in connection with any determination of the consumer's eligibility, or continued eligibility, for credit without specifically requesting medical information. The rule of construction is retained as an interpretation, rather than as an exception because it interprets the statutory language regarding when a creditor ''obtains'' medical information in violation of the prohibition.

The introductory language to the rule of construction has been revised for clarity to provide that a creditor does not obtain medical information ''in violation of the prohibition'' if it meets the specified criteria. In addition, the cross-reference to the general prohibition has been deleted because the rule of construction is an interpretation of the statute.

Proposed paragraph (b)(1)(ii), which prohibited the use of unsolicited medical information, has been deleted because the rule of construction focuses on when a creditor does not obtain medical information in violation of the statute. The Agencies believe that incorporating a use limitation in the rule of construction would be

inconsistent with the exceptions in renumbered paragraphs (d) and (e). Instead, the Agencies have added a new paragraph (c)(2) to clarify that a creditor that receives unsolicited medical information may use that information in connection with any determination of the consumer's eligibility, or continued eligibility, for credit only to the extent the creditor can rely on one of the exceptions in renumbered paragraphs (d) or (e).

The examples of the rule of construction have been moved to renumbered paragraph (c)(3) in the interim final rules and all references to restrictions on the use of unsolicited medical information have been deleted from the examples consistent with the changes discussed above. In addition, paragraph (c)(3)(iii) adds a new example to illustrate how the rule of construction applies to medical information furnished by a consumer reporting agency.

Commenters had several other comments concerning the rule of construction. Privacy advocates, consumer and community groups, and health care associations suggested that the Agencies clarify that the phrase ''without specifically requesting medical information'' means information obtained voluntarily without any pressure, prompting, or direct or indirect solicitation by the creditor. These commenters also sought an additional requirement that creditors destroy unsolicited medical information as soon as reasonably practicable and suggested making the rule of construction an exception. Some industry commenters suggested that consumers should have the burden of proving that unsolicited medical information was used in a credit eligibility determination because it may be difficult for creditors to prove that unsolicited medical information was not used. Some industry commenters suggested permitting a creditor to use unsolicited medical information in a manner no less favorably than it would use comparable medical information.

The statute does not specifically address the burden of proof to be applied when disputes arise regarding the use of medical information. The Agencies find it unnecessary to address this issue because the interim final rule allows unsolicited medical information to be used as permitted by the exceptions in renumbered paragraphs (d) and (e). The Agencies thus decline to impose on consumers the burden of proving that unsolicited medical information was used in a credit eligibility determination. Furthermore, even if the consumer requests that a creditor use unsolicited medical information in connection with a credit eligibility determination, the creditor is not required to do so. The phrase ''without specifically requesting medical information'' along with the examples makes clear that the rule of construction does not apply to medical information obtained through a specific request or solicitation for such information. No further clarification is necessary. The destruction of unsolicited medical information would not be appropriate in many circumstances, thus the Agencies decline to adopt such a rule.

D. Financial Information Exception for Obtaining and Using Medical Information

As noted above, section 604(g)(5)(A) of the Act gives the Agencies the authority to prescribe regulations, after notice and opportunity for comment, to permit transactions in which creditors may obtain and use medical information in connection with determinations of credit eligibility that the Agencies determine to be necessary and appropriate to protect legitimate operational, transactional, risk, consumer, and other needs (including actions necessary for administrative verification purposes), consistent with the intent of the statute to restrict the use of medical information for inappropriate purposes. Applying this standard, the Agencies proposed a number of exceptions to the general prohibition on creditors obtaining or using medical information in connection with credit eligibility determinations. The exceptions were contained in proposed paragraphs (c)–(d). In the interim final rule, these exceptions are contained in renumbered paragraphs (d) and (e) of each Agency's rule and in §§ __.3 and __.4 of the separate rule.

Section __.30(c) of the proposal contained the proposed financial information exception. Proposed paragraph (c)(1) provided that a creditor may obtain and use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit so long as the following three elements were met. First, the information must relate to debts, expenses, income, benefits, collateral, or the purpose of the loan, including the use of proceeds. Second, the creditor must use the information in a manner and to an extent no less favorable than it would use comparable information that is not medical information in a credit transaction. Third, the creditor must not take the consumer's physical, mental, or behavioral health, condition or history, type of treatment, or prognosis into account as part of any such determination of credit eligibility.

Commenters generally supported the proposed three-part test for the financial information exception. Privacy advocates, consumer and community groups, and health care associations suggested limiting the exception to circumstances where the creditor has not specifically requested medical information on its application for credit, but rather has made a generic request for financial information. These commenters also suggested including the phrase ''financial information'' in the text of the rule. Industry commenters suggested revising the first prong to apply to a non-exclusive list of information routinely used in the underwriting process. These commenters noted that the Agencies may have unintentionally omitted certain items, such as assets, that should be included in the list. Commenters generally supported the second prong of the test. One commenter suggested that the third prong of the test was inconsistent with and undermined the ''no less favorable'' principle set forth in the second prong and could prove detrimental to consumers. Another commenter found the three-part test complicated and difficult to implement.

The interim final rule retains the three-part test for the financial information exception, with certain modifications. The Agencies agree with those commenters that believe the better approach is to have a non-exclusive list of types of information that are routinely used in making credit eligibility determinations. The first prong of the test, therefore, has been revised to include all information of the type routinely used in making credit eligibility determinations and provides a non-exclusive list of such types of information (*i.e.*, information relating to debts, expenses, income, benefits, assets, collateral, or the purpose of the loan, including the use of proceeds). The Agencies do not believe it would be helpful to include the words ''financial information'' in the text of the exception because there is no bright line between financial information and medical information.

The second prong of the test is adopted as proposed. Commenters appeared comfortable with requiring a creditor to use medical information in a manner and to an extent no less favorable than it would use comparable non-medical information in a credit transaction. As noted in the proposal, a creditor may deny credit to the

consumer because the consumer owes a debt to a hospital if the creditor would have denied credit to the consumer if the consumer had owed the same amount of debt with the same payment history to a retailer. Nothing in the rule prevents the creditor from treating information about medical debts (or expenses or income) more favorably than non-medical debts.

The third prong of the test is also adopted as proposed. Other, more narrowly focused exceptions, such as the medical accommodation exception, permit a creditor to take the consumer's physical, mental, or behavioral health, condition, or history, type of treatment, or prognosis into account in limited circumstances as part of a consumer's credit eligibility determination. For this type of core medical information, the Agencies believe it is appropriate to more strictly limit the circumstances in which creditors may obtain or use this information.

Since creditors generally are prohibited from obtaining medical information in connection with any determination of the consumer's eligibility, or continued eligibility, for credit, a creditor ordinarily would not specifically request medical information on an application, but would obtain such information in response to a generic question on an application about debts, income, and other information routinely used in credit eligibility determinations. Thus, except where a creditor has a specific application for the financing of medical procedures, a creditor generally would be prohibited from specifically asking for medical information on a credit application.

Proposed paragraph (c)(2) provided several non-exclusive examples to illustrate when creditors may obtain and use medical information under the financial information exception. Commenters generally supported the proposed examples. One commenter requested a clarification of the example in proposed paragraph (c)(2)(iii)(B). In that example, a consumer meets with a loan officer of a creditor to apply for a mortgage loan. While filling out the loan application, the consumer informs the loan officer orally that she has a potentially terminal disease. The consumer meets the creditor's established requirements for the requested mortgage loan. The loan officer recommends to the credit committee that the consumer be denied credit because the consumer has that disease. The commenter recommended adding a statement that the bank acted on the loan officer's recommendation and denied the application because the consumer had a potentially terminal disease to clarify that the creditor, in fact, used medical information in a manner inconsistent with the exception. The Agencies believe this clarification is helpful and, in the interim final rule, have revised the example in renumbered paragraph (d)(2)(iii)(B) of each Agency's rule accordingly. *See also* section __.3(b)(3)(ii) of the separate rule.

In addition, a new example has been added in paragraph (d)(2)(iii)(C) of each Agency's rule and § __.3(b)(3)(iii) of the separate rule to illustrate that a creditor cannot use a consumer's apparent medical condition as the basis for requiring the consumer to obtain debt cancellation, debt suspension, or credit insurance coverage as a condition for the extension of credit. Even though the use of medical information to determine the consumer's eligibility for a debt cancellation contract, debt suspension agreement, or credit insurance product generally is subject to an exception to the general prohibition pursuant to paragraphs (e)(1)(viii) or (e)(1)(ix), a creditor may not condition an extension of credit to the consumer on the consumer obtaining debt cancellation, debt suspension, or credit insurance coverage based on the consumer's physical, mental, or behavioral health, condition or history, type of treatment, or prognosis.

In addition, the heading of renumbered paragraph (d)(2)(i) has been revised in the interim final rule to reflect changes made to the first prong of the test to encompass the type of information routinely used in making credit eligibility determinations. Non-substantive revisions have also been made to the examples in renumbered paragraphs (d)(2)(ii)(A) and (C) for clarity. Aside from these changes, the examples are adopted as proposed.

E. Specific Exceptions for Obtaining and Using Medical Information

Section __.30(d) of the proposal contained a number of specific exceptions to the general prohibition. These exceptions would allow creditors to obtain and use medical information for a limited number of particular purposes in connection with a determination of the consumer's eligibility, or continued eligibility, for credit. A creditor that obtains medical information pursuant to one of these specific exceptions may not subsequently use the information in connection with determining the consumer's eligibility, or continued eligibility, for credit unless an exception applies. In the interim final rule, the specific exceptions are contained in renumbered paragraph (e) of each Agency's rule. Section __.4 of the separate rule contains the identical exceptions in paragraphs (a)(1)–(9).

Determination of power of attorney, legal representative and legal capacity. Proposed paragraph (d)(1)(i) provided that a creditor may obtain and use medical information to determine whether the use of a power of attorney or legal representative is necessary and appropriate. This exception was designed to permit a creditor to verify, in connection with a credit eligibility determination, that the exercise of a power of attorney or legal representative is necessary and appropriate. Some industry commenters suggested that the exception clarify that creditors may obtain and use medical information to determine the consumer's competency or legal capacity to contract. Privacy advocates, consumer and community groups, and health care associations suggested limiting the power of attorney exception to circumstances where a power of attorney is triggered by a medical condition or where there is a legitimate question about the consumer's legal capacity to contract when a person asserts the exercise of a power or attorney or claims to act as a legal representative on behalf of a consumer. The FTC commented that the limited circumstances where medical information may be obtained and used to determine whether a power of attorney is necessary and appropriate would not be in connection with a credit eligibility determination, and therefore should be addressed through an interpretation of the statute, rather than through an exception.

The interim final rule revises the exception for the use of a power of attorney or legal representative. Renumbered paragraph (e)(1)(i) of the interim final rule permits a creditor to obtain and use medical information in connection with determining the consumer's credit eligibility to determine whether the use of a power of attorney or legal representative that is triggered by a medical event or condition is necessary and appropriate or whether the consumer has the legal capacity to contract when a person seeks to exercise a power of attorney or act as legal representative for a consumer based on an asserted medical event or condition. The interim final rule makes two substantive changes in response to the comments received. First, the exception has been narrowed to permit a creditor to obtain and use medical information only when the power of attorney or legal representative is triggered by a medical event or condition. Second, the exception has been revised to permit a creditor to

determine whether the consumer has the legal capacity to contract where a person seeks to exercise a power of attorney or act as a legal representative based on an asserted medical event or condition. This revision is designed to clarify that creditors may obtain and use medical information to verify that the asserted medical event or condition triggering the power of attorney or legal representative has, in fact, occurred and renders the consumer legally incapable of contracting. Where use of a power of attorney or legal representative is triggered by non-medical events or conditions, creditors should not need to obtain or use medical information.

In response to the FTC's comments, the Agencies recognize that a power of attorney or legal representative may be used in a variety of circumstances, many of which have no connection with a determination of a consumer's eligibility, or continued eligibility, for credit. For example, a power of attorney or legal representative may be used in connection with establishing a deposit or other asset account. In those circumstances, the general prohibition on obtaining or using medical information would not apply because the information would not be obtained or used in connection with any determination of the consumer's eligibility, or continued eligibility, for credit. The introductory language to renumbered paragraph (e) of the interim final rules makes clear that the specific exceptions apply to a creditor that ''may obtain and use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit.'' A creditor that obtains and uses medical information in circumstances not connected with a credit eligibility determination is not subject to the general statutory prohibition and does not have to rely upon the power of attorney or any other exception.

Compliance with applicable law. Proposed paragraph (d)(1)(ii) provided an exception to permit a creditor to obtain and use medical information to comply with applicable requirements of local, state, or Federal laws. The Agencies received only a few comments on this proposed exception. One commenter asked the Agencies to clarify that this exception covered laws that prohibit unfair and deceptive acts or practices. The FTC suggested that the financial abuse statutes referenced in the preamble as an example do not involve credit eligibility determinations, and therefore a statutory interpretation was more appropriate than an exception.

In the interim final rule, renumbered paragraph (e)(1)(ii) is adopted as proposed. Although many legal requirements do not have any connection with credit eligibility, other laws may have such a connection. As noted above, a creditor that obtains and uses medical information to comply with applicable laws in circumstances that are not connected with a credit eligibility determination is not subject to the general statutory prohibition and does not have to rely upon the exception. However, the exception is retained to cover those circumstances where it may be needed to protect creditors from inconsistent legal obligations.

Special credit program or credit-related assistance program. One commenter suggested that the proposed compliance with applicable laws exception would not be sufficient to permit creditors to obtain and use medical information in connection with special credit or credit-related programs, such as programs established by government-sponsored enterprises. Such programs may require creditors as part of the program requirements to obtain and use medical information in ways not covered by the other exceptions. Consistent with the policy goals established by Congress, the prohibition on creditors obtaining or using medical information should not interfere with the ability of creditors to assist consumers to qualify for beneficial special programs established by government-sponsored enterprises, not-for-profit organizations, or others.

To address this concern, the interim final rule contains a new exception in renumbered paragraph (e)(1)(iii) that permits creditors to obtain and use medical information in connection with a determination of the consumer's eligibility, or continued eligibility, for credit, to determine, at the consumer's request, whether the consumer qualifies for a legally permissible special credit program or credit-related assistance program that is: (a) Designed to meet the special needs of consumers with medical conditions and (b) established and administered pursuant to a written plan of the plan sponsor that identifies the class of persons that the program is designed to benefit and sets forth the procedures and standards for extending credit or providing other credit-related assistance under the program. Because not all potentially eligible consumers may seek to qualify for a special credit or credit assistance program, this exception applies only when the consumer requests to be considered for the program. A creditor, however, may provide consumers with information about such programs to educate consumers about their options. In addition, any special credit or credit assistance program must meet the requirements of all applicable fair lending laws. The plan sponsor may include a government agency, charitable organization, the creditor, or any other person. This exception is modeled after the provisions relating to special purpose credit programs in the ECOA and the Board's Regulation B, 12 CFR part 202. What programs are permissible and what inquiries to determine medical eligibility are permissible, however, are governed by other laws, including applicable fair lending laws, and are beyond the scope of this rule.

Renumbered paragraph (e)(2) of the interim final rule provides an example to illustrate this exception. In the example, a not-for-profit organization establishes a credit assistance program pursuant to a written plan that is designed to assist disabled veterans purchase homes by subsidizing the down payment for the home purchase mortgage loans of qualifying veterans. The organization works through mortgage lenders and requires mortgage lenders to obtain medical information about the disability of any consumer that seeks to qualify for the program, use that information to verify the consumer's eligibility for the program, and forward that information to the organization. A consumer who is a veteran applies to a creditor for a home purchase mortgage loan. The creditor informs the consumer about the credit assistance program for disabled veterans and the consumer seeks to qualify for the program. The example states that, assuming that the program complies with all applicable law, including applicable fair lending laws, the creditor may obtain and use medical information about the medical condition and disability, if any, of the consumer to determine whether the consumer qualifies for the credit assistance program.

Fraud prevention or detection. Proposed paragraph (d)(1)(iv) provided that a creditor may obtain and use medical information for purposes of fraud prevention and detection. Industry commenters supported the proposed exception. Privacy advocates, consumer and community groups, and health care associations believed the proposed exception was overbroad and unnecessary in light of the other exceptions.

The interim final rule retains the fraud prevention or detection exception in renumbered paragraph (e)(1)(iv), although the language has been revised to make clear that the exception is

available only to the extent necessary to prevent or detect fraud. The Agencies anticipate that creditors would find it necessary to obtain and use medical information for purposes of fraud prevention and detection in limited circumstances. Creditors relying on this exception should have the systems in place to demonstrate the necessity for obtaining and using medical information to prevent or detect fraud. Creditors that actually use medical information in legitimate fraud prevention or detection programs should be able to make this demonstration. Blanket assertions of a fraud prevention or detection purpose alone, however, are not sufficient to justify the collection of medical information about consumers under the anti-fraud exception.

Financing medical products or services. Proposed paragraph (d)(1)(v) provided that a creditor may obtain and use medical information in connection with credit eligibility determinations in the case of credit for the purpose of financing medical products or services to determine and verify the medical purpose of a loan and the use of proceeds. As noted in the proposal, certain creditors have established specialized loan programs that finance specific medical procedures, such as vision correction surgery, but not others. In such cases, the creditor may need to obtain and use medical information in connection with determining whether the purpose of the loan is within the scope of the creditor's established loan program. The proposal also provided examples of this exception.

Commenters generally supported the medical financing exception. Several commenters suggested revising the example in proposed paragraph (d)(2)(i) to permit the creditor to verify that the procedure to be financed will be performed, in conformance with the language of the exception, rather than permitting a creditor to confirm the consumer's medical eligibility.

Renumbered paragraph (e)(1)(v) of the interim final rule retains the medical financing exception as proposed. The examples of the medical financing exception have been moved to paragraph (e)(3) in the interim final rule. The example in paragraph (e)(3)(i) of the interim final rule has been revised from the proposal in accordance with the commenters' suggestions.

Medical accommodation. Section __.30(d)(1)(vi) of the proposal provided that a creditor may obtain and use medical information if the consumer or the consumer's legal representative requested in writing, on a separate document signed by the consumer or the consumer's legal representative, that the creditor use specific medical information for a specific purpose in determining the consumer's eligibility, or continued eligibility, for credit, to accommodate the consumer's particular circumstances. Under the proposal, the signed, written request had to describe the specific medical information that the consumer requested the creditor to use and the specific purpose for which the information would be used. The proposal contemplated an individualized process in which the consumer would inform the creditor about the specific medical information that the consumer would like the creditor to use and for what purpose. As noted in the preamble to the proposal, this exception was not intended to allow creditors to obtain consent on a routine basis or as a part of loan applications or documentation. The proposal provided examples of the medical accommodation exception.

Commenters had a number of recommendations regarding the medical accommodation exception. Privacy advocates, consumer and community groups, and health care associations suggested that the regulation should explicitly state that creditors may not request medical information or consent to obtain medical information on a routine basis or as part of a loan application. Several commenters also suggested clarifying that the request must be voluntary and initiated by the consumer. In addition, commenters suggested including language in the regulation to clarify that the exception is not met by a form that contains a pre-printed description of various types of medical information and the uses to which it might be put. Some commenters urged the Agencies to add a disposal requirement on creditors that obtain information that is not needed. Consumer and community groups also suggested eliminating the forbearance interpretation, folding that interpretation into the medical accommodation exception, and adding anti-discrimination protections to the provision, similar to the ''no less favorable'' standard used in renumbered paragraph (d).

Industry commenters generally believed that the medical accommodation was too restrictive. Some industry commenters suggested that the use of pre-printed consent forms or other routine form of consent should be sufficient to trigger the exception. Other commenters suggested that the consumer should be able to request the use of medical information through oral and electronic means, not simply through a signed writing. One commenter noted that many creditors include a section on their credit applications where the consumer may describe special circumstances or other information that the consumer would like the creditor to consider. This commenter recommended relaxing the requirements of the medical accommodation exception to enable the exception to apply in this circumstance. Another commenter noted that the medical accommodation exception was drafted so narrowly that it may prohibit a creditor from obtaining or using additional medical information to verify or corroborate the facts necessary to support a consumer's medical accommodation request.

In the interim final rule, the medical accommodation exception in renumbered paragraph (e)(1)(vi) has been revised to address commenters' concerns. Paragraph (e)(1)(vi) provides an exception for circumstances where the consumer or the consumer's legal representative specifically requests that the creditor use medical information in determining the consumer's eligibility, or continued eligibility, for credit, to accommodate the consumer's particular circumstances, and such request is documented by the creditor. Any such accommodation must be consistent with safe and sound practices. The requirement for a separate signed writing by the consumer that describes the specific medical information and the specific purpose for which it is to be used has been deleted in the interim final rule. Instead, the interim final rule focuses on the specific request of the consumer and the creditor's documentation of that request. As revised, the interim final rule permits the medical accommodation exception to be triggered by the consumer's oral, electronic, or written request. A consumer may make a specific request by responding to a generic inquiry on a credit application that invites the consumer to describe any special circumstances or other information (not limited to medical information) that the consumer would like the creditor to consider in evaluating the consumer's application. The disposal of records connected with a specific request for a medical accommodation is beyond the scope of this rule and may not be appropriate in certain circumstances.

The proposal contained examples to illustrate the medical accommodation exception. In the interim final rule, the examples have been moved to paragraph (e)(4) and revised and expanded to address commenters' concerns.

By its terms, the medical accommodation exception incorporates a non-discrimination provision, because

a creditor may only use medical information to ''accommodate'' or favor the consumer's particular circumstances. Using medical information to discriminate against or disadvantage the consumer would not meet the requirements of the exception. Nothing in this rule, however, requires a creditor to consider medical information at the consumer's request or to provide an accommodation to the consumer. Under this rule, a creditor may disregard medical information obtained in connection with a consumer's specific request for an accommodation and evaluate the consumer in accordance with the creditor's otherwise applicable underwriting criteria. Other applicable laws, including applicable fair lending laws, may require creditors to consider such requests in certain circumstances. Consideration of circumstances governed by other applicable laws is beyond the scope of this rule. The example in renumbered paragraph (e)(4)(i) has been revised to clarify the creditor's options when presented with a specific request from a consumer for a medical accommodation.

The example in renumbered paragraph (e)(4)(ii) has been revised to apply to a specific request made by telephone and documented by the creditor. The example in paragraph (e)(4)(iii) is new and illustrates how a specific request may be made by the consumer on a credit application.

A consumer who specifically requests a medical accommodation may not provide sufficient information to enable a creditor to determine whether such an accommodation is warranted. In that case, a creditor may request additional information as necessary to verify or corroborate the information provided or to enable the creditor to determine whether to make a medical accommodation for the consumer's particular circumstances. The consumer at any time may decline to provide further medical information, withdraw the request for an accommodation, and choose to be evaluated according to the creditor's otherwise applicable underwriting criteria. The example in paragraph (e)(4)(iv) is new and illustrates how creditor requests for additional information may be handled.

As noted in the proposal, creditors may not rely on the medical accommodation exception to routinely obtain and use medical information about consumers in connection with credit eligibility determinations. This exception is triggered when the consumer specifically requests an accommodation. The requirement for a specific request from the consumer is not satisfied by a creditor routinely including boilerplate language in a credit application which indicates that by applying for credit the consumer authorizes or consents to the creditor obtaining and using medical information in connection with credit eligibility determinations. The example in paragraph (e)(4)(v) is new and illustrates that routine requests by creditors do not fall within the exception.

Forbearance. In the proposal, forbearance practices and programs were addressed as an interpretation, rather than as an exception. Industry commenters believed that the proposed interpretation was too narrow because it only covered the triggering of forbearance practices and programs. These commenters believed that medical information should be available for use in determining whether to offer forbearance practices or programs to the consumer. Several industry commenters also requested clarification that informal forbearance practices would be covered by this interpretation. Privacy advocates, consumer and community groups, and health care associations suggested limiting the proposed interpretation to forbearance practices and programs triggered by a medically related event.

In the interim final rule, forbearance practices and programs are addressed in a new exception in paragraph (e)(1)(vii). Forbearance practices and programs may be established to address both medical and non-medical events. The exception, however, applies only to forbearance practices and programs that are triggered by medical events or conditions. Accordingly, paragraph (e)(1)(vii) of the interim final rule creates an exception to permit creditors to obtain and use medical information ''consistent with safe and sound practices, to determine whether the provisions of a forbearance practice or program that is triggered by a medical event or condition apply to a consumer.'' This exception is flexible enough to cover both formal and informal forbearance practices and programs. Application of a forbearance practice or program may or may not be based on the request of the consumer. Paragraph (e)(5) provides an example of a forbearance practice or program.

Debt cancellation contracts, debt suspension agreements, or credit insurance products. As noted above, the proposal addressed debt cancellation contracts, debt suspension agreements, and credit insurance products through an interpretation. Most commenters believed that it was more appropriate to address these contracts, agreements, and products through an exception. The FTC, however, recommended that the Agencies continue to address debt cancellation contracts, debt suspension agreements, and credit insurance products through an interpretation. The Agencies believe that the better approach is to create exceptions and, thus, have created two new exceptions in paragraphs (e)(1)(viii) (covering debt cancellation contracts and debt suspension agreements) and (e)(1)(ix) (covering credit insurance products) for the reasons discussed below.

Industry commenters believed that the proposed interpretation was too narrow because it only covered the triggering of debt cancellation contracts, debt suspension agreements, and credit insurance products. These commenters believed that medical information should be available for use in determining the consumer's eligibility for, the triggering of, or the reactivation of those contracts, agreements, or products. Privacy advocates, consumer and community groups, and health care associations believed that the proposed interpretation was too broad because debt cancellation contracts and debt suspension agreements are often triggered by events such as loss of employment or divorce that have no connection with medical information. Privacy advocates, consumer and community groups, and health care associations urged the Agencies to delete credit insurance from the proposed provision, maintaining that creditors typically do not offer credit insurance directly. Industry commenters had various suggestions regarding credit insurance, including creating a separate exception for credit insurance, referencing credit insurance in the preceding paragraph (a)(2)(i)(A) (now paragraph (b)(2)(iii)(A)), or broadening the proposed interpretation to cover eligibility and reactivation determinations.

In the interim final rule, debt cancellation contracts and debt suspension agreements are addressed in one exception (paragraph (e)(1)(viii)) and credit insurance products are addressed in a separate exception (paragraph (e)(1)(ix)) in recognition of the distinct character of those products. *See also* sections __.4(a)(8) and (9) of the separate rule.

Under this rule, a creditor may not use medical information about a consumer to determine whether the consumer will be required to obtain a debt cancellation contract, debt suspension agreement, or credit insurance product. For example, a consumer who is in a wheelchair cannot be required to obtain credit insurance

because of the consumer's disability. An example in paragraph (d)(2)(iii)(C) of each Agency's rule and in § __.3(b)(3)(iii) of the separate rule illustrates this limitation. Also, a creditor would not violate this particular rule if it requires all consumers who seek a particular type of credit, such as credit to finance the purchase of a home with a small down payment, to obtain credit insurance or a similar product.

The rule makes clear that creditors may use medical information to underwrite credit insurance, or to underwrite related credit products, such as debt cancellation contracts and debt suspension agreements, if a medical condition or event is a triggering event for the provision of benefits. However, denial of these products cannot be used as a subterfuge to consider medical information in making a determination about eligibility or continued eligibility for the underlying loan.

In addition, other laws and regulations, including applicable anti-tying rules and fair lending laws, may prohibit or otherwise restrict a creditor from requiring a consumer to obtain a debt cancellation contract, debt suspension agreement, or credit insurance product in connection with an extension of credit.[10] A discussion of the circumstances prohibited by other laws and regulations is beyond the scope of this rule.

Finally, creditors are reminded that when a creditor offers a consumer a debt cancellation contract, debt suspension agreement, or credit insurance product that is related to a credit product that the consumer obtains or seeks to obtain from the creditor, it may not be clear to the consumer why the creditor is seeking to obtain medical information. As discussed below, creditors generally would be prohibited from specifically asking for medical information on a credit application, except where a creditor has a specific application for the financing of medical procedures. Whether medical information is collected on the credit application or through other means, creditors should make it clear to consumers that the purpose for obtaining medical information relates to debt cancellation contracts, debt suspension agreements, or credit insurance products, rather than to the credit itself. Moreover, where obtaining those products is voluntary, the consumer should be told that it is not necessary to provide medical information and that the failure to answer medically related questions will have no impact on the credit decision.

Deleted exceptions and additional exceptions requested by commenters. Proposed paragraph (d)(1)(iii) provided that a creditor may obtain and use uncoded medical information included in a consumer report furnished by a consumer reporting agency in accordance with section 604(g)(1)(B) of the FCRA, if such information is used for the purpose for which the consumer provided specific written consent. As discussed above, this proposed exception has been eliminated.

Proposed paragraph (d)(1)(vii) provided that a creditor may obtain and use medical information as otherwise permitted by order of the appropriate agency. Privacy advocates, consumer and community groups, and health care associations objected to this provision. The Agencies believe this paragraph is unnecessary and have omitted it from the interim final rule because the Agencies are adopting identical exceptions and, as noted above, intend to make any amendments to the rules in consultation and coordination with each other.

Commenters also requested the creation of a number of additional exceptions for flexible spending programs tied to credit cards, for products tied to a consumer's life expectancy, and to facilitate resolution of direct disputes with consumers. The Agencies believe that additional exceptions are not needed and that commenters' concerns are adequately addressed by the interpretation of ''eligibility, or continued eligibility, for credit'' and the existing exceptions.

Section __.31 Limits on Redisclosure of Information

Proposed section __.30(e) incorporated the statutory provision regarding the limits on redisclosure of medical information. In the proposal, this paragraph provided that a person that receives medical information about a consumer from a consumer reporting agency or an affiliate is prohibited from disclosing that information to any other person, except as necessary to carry out the purposes for which the information was initially disclosed, or as otherwise permitted by statute, regulation, or order.

Some commenters requested clarification of the phrase ''as otherwise permitted by statute, regulation, or order'' that is used in the statute and proposed regulation. Other commenters requested clarification that a redisclosure may be made for any purpose described in section 502(e) of the GLB Act. The Agencies believe that the redisclosure language, which was taken directly from the statute, is clear and that no further clarification is necessary.

In the interim final rules, the Agencies are adopting this provision in a new section __.31 in each Agency's rule pursuant to their joint rulemaking authority under section 621(e) of the FCRA. The separate rule does not contain a similar provision on redisclosure limits.

Section __.32 Sharing Medical Information With Affiliates

Section __.31 of the proposal addressed the sharing of medically related information with affiliates. In the interim final rule, these provisions are contained in section __.32.

Proposed paragraph (a) provided that the standard exclusions from the definition of ''consumer report'' contained in section 603(d)(2) of the Act—including the exclusions for sharing transaction or experience information among affiliates or sharing other eligibility information among affiliates after notice and an opportunity to opt-out—do not apply if medical information, an individualized list or description based on payment transactions for medical products or services, or an aggregate list or description based on payment transactions for medical products or services is disclosed to an affiliate.

Proposed paragraph (b) provided that the special restrictions on sharing medically related information with affiliates did not apply, and the standard exclusions from the definition of consumer report remained in effect, if the information was disclosed to an affiliate in certain circumstances. The proposal incorporated each of the exceptions enumerated in section 604(g)(3)(A) and (B) of the Act.

The first statutory exception is when medically related information is shared with an affiliate in connection with the business of insurance or annuities (including the activities described in section 18B of the model Privacy of Consumer Financial and Health Information Regulation issued by the National Association of Insurance Commissioners (NAIC), as in effect on January 1, 2003). Some commenters questioned the adequacy of the comment period based on the fact that the NAIC model privacy regulation is

[10] For example, banks are prohibited from conditioning an extension of credit on the consumer obtaining some additional credit, property or service from the bank or its affiliate other than a loan, discount, deposit or trust service, *see* Bank Holding Company Amendments of 1970 § 106(b) (12 U.S.C. 1972); *see also* 12 CFR 37.3(a) (providing that a national bank may not extend credit nor alter the terms or conditions of an extension of credit conditioned upon the customer entering into a debt cancellation contract or debt suspension agreement with the bank).

not readily available to the public, but must be purchased from NAIC. The reference to the NAIC model privacy regulation is a statutory reference that the Agencies have incorporated into the regulation. Interested parties may purchase a copy of the NAIC model Privacy of Consumer Financial and Health Information Regulation at *http://www.naic.org.*

The second statutory exception is when medically related information is shared with an affiliate for any purpose permitted without authorization under the Standards for Individually Identifiable Health Information promulgated by the Department of Health and Human Services (HHS) pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). One commenter asked the Agencies to broaden this exception by deleting the phrase ''for any purpose permitted without authorization'' and replacing it with a reference to any sharing ''as permitted under'' the HIPAA regulations issued by HHS. The Agencies find no basis for altering the specific exceptions adopted by Congress. Furthermore, the Agencies note that the special affiliate sharing restrictions do not apply unless the communication of medically related information would otherwise meet the definition of a ''consumer report.''

The third statutory exception is when medically related information is shared with an affiliate for any purpose referred to under section 1179 of HIPAA. Section 1179 of HIPAA provides that to the extent that an entity is engaged in activities of a financial institution or is engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling or collecting payments for a financial institution, the HIPAA standards and requirements do not apply to the entity with respect to such activities. Section 1179 also provides as an example of a use or disclosure of information not covered by that statute, the use or disclosure of information for authorizing, processing, clearing, settling, billing, transferring, reconciling, or collection, a payment for, or related to, health care premiums or health care. Some commenters requested that the Agencies contact the Department of Health and Human Services (HHS) to clarify an issue regarding the scope of section 1179. Any consultation with HHS regarding section 1179 of HIPAA would be independent of this rulemaking.

The fourth statutory exception is when medically related information is shared with an affiliate for any purpose described in section 502(e) of the GLB Act. As previously noted in the proposal, some of the purposes described in section 502(e) of the GLB Act may be germane to the sharing of information among affiliates—for example, sharing with the consent of the consumer, for fraud prevention purposes, or as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer—while other purposes described in section 502(e) are not—for example, sharing information with law enforcement or regulatory authorities.

The fifth exception is not set forth in the statute and provides that the special restrictions on sharing medically related information with affiliates do not apply, and the standard exclusions from the definition of consumer report remain in effect, if the information is disclosed to an affiliate in connection with a determination of the consumer's eligibility, or continued eligibility, for credit consistent with § __.30 of this subpart. Industry commenters supported this exception. Privacy advocates, consumer and community groups, and health care associations requested the deletion of this exception or, as an alternative, that this exception not apply to uncoded medical information obtained from a consumer reporting agency with the consumer's specific written consent or to information obtained pursuant to the medical accommodation exception. This exception is adopted as proposed in paragraph (b)(5).

The Agencies continue to believe that it is necessary and appropriate to allow a person to share medically related information with an affiliate in connection with a determination of the consumer's eligibility, or continued eligibility, for credit consistent with the provisions of § __.30. In response to commenters' concerns, the Agencies note that the interim final rule permits uncoded medical information from a consumer reporting agency to be used only as permitted by the exceptions in § __.30(d) and (e). Moreover, the medical accommodation exception restricts creditors from routinely obtaining and using medical information because the exception is triggered by a consumer's specific request. Thus, the Agencies believe that the provisions of § __.30(d) and (e) are sufficient to prevent the inappropriate sharing of medical information with and the inappropriate use of medical information by affiliates.

Finally, the sixth exception provides that the special restrictions on sharing medically related information with affiliates would not apply if otherwise permitted by order of the appropriate agency. This exception incorporates the authority delegated to the Agencies by the Congress to create exceptions through orders. Privacy advocates, consumer and community groups, and health care associations acknowledged the authority of the Agencies to expand the affiliate-sharing exceptions by order. This exception is adopted as proposed in paragraph (b)(6).

As noted in the proposal, the prohibitions on obtaining or using medical information in § __.30 operate independently from the exceptions that permit the sharing of that information among affiliates in accordance with the provisions of section 603(d)(2) of the Act. For example, if a mortgage lender has obtained and used medical information in accordance with one of the exceptions in § __.30(c) or (d), the mortgage lender may share that information with its credit card affiliate without becoming a consumer reporting agency if one of the exceptions in § __.32(b) applies. However, the credit card affiliate may not obtain or use that information in connection with any determination of the consumer's eligibility, or continued eligibility, for credit, except to the extent permitted by § __.30.

Effective Date and Solicitation of Comments

The statute provides that the final rules shall take effect on the later of 90 days after the rules are issued in final form, or the date specified in the regulations. Commenters believed that the effective date of the final rules should be no sooner than 90 days after the rules are issued in final form, although many commenters requested a longer period before the final rules take effect. Commenters generally believed that the effective date should be synchronized with the statutory prohibition, so that creditors would not be subject to the prohibition on obtaining or using medical information before the effective date of the regulatory exceptions. The interim final rules shall take effect on March 7, 2006, which is 270 days after the date of publication in the **Federal Register**. Comments on the interim final rule must be received by July 11, 2005.

V. Regulatory Analysis

Paperwork Reduction Act

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3506, *et seq.*) and its implementing regulations at 5 CFR part 1320, including Appendix A.1, the Agencies have reviewed the interim final rules and determined that they contain no collections of information. The Board

made this determination under authority delegated by the Office of Management and Budget.

Regulatory Flexibility Analysis

OCC: The OCC received no comment on its Initial Regulatory Flexibility Analysis published in connection with the April 28, 2004, NPRM. Upon further review, the OCC certifies that this interim final rule will not have a significant economic impact on a substantial number of small entities.

Under section 605(b) of the Regulatory Flexibility Act (RFA), 5 U.S.C. 605(b), the regulatory flexibility analysis otherwise required under section 604 of the RFA is not required if an agency certifies, along with a statement providing the factual basis for such certification, that the rule will not have a significant economic impact on a substantial number of small entities. The OCC has reviewed the impact of this interim final rule on small entities and certifies that it will not have a significant economic impact on a substantial number of small entities.

The Small Business Administration (SBA) has defined ''small entities'' for banking purposes as a bank or savings institution with assets of $150 million or less. *See* 13 CFR 121.201. The interim final rule implements section 411 of the FACT Act and imposes only minimal economic impact on national banks. The interim final rule creates exceptions to the FACT Act's prohibition against national banks obtaining and using a consumer's medical information in connection with credit determinations. Additionally, the interim final rule implements the FACT Act's restrictions on the sharing of medical information among affiliates and includes exceptions to permit the sharing of medical information in certain circumstances. The interim final rule applies to national banks, Federal branches and agencies, their respective subsidiaries, and persons that participate in a credit transaction involving a national bank, Federal Branch or agency, or their respective subsidiaries (''entities'') that obtain or use medical information in connection with credit determinations, regardless of their size. However, it is likely that small entities, because of the nature and size of their operations, will encounter fewer instances where they might obtain or use medical information. Therefore, the interim final rule is not expected to result in a significant economic impact for small national entities.

Board: The Board has prepared a final regulatory flexibility analysis as required by the Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*).

1. *Statement of the need for and objectives of the interim final rule.* The FACT Act amends the FCRA and was enacted, in part, for the purpose of protecting consumers' medical information. Section 411 of the FACT Act contains a general prohibition on creditors obtaining or using medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit. Section 411 authorizes the Board, together with the other Agencies, to create exceptions to allow creditors to obtain or use medical information for eligibility purposes where necessary and appropriate to protect legitimate operational, transactional risk, consumer, and other needs, consistent with the Congressional intent to restrict the use of medical information for inappropriate purposes.

Section 411 also limits the ability of an institution to share medical information with its affiliates without becoming a consumer reporting agency, subject to certain exceptions, and restricts the redisclosure of medical information. The statute authorizes the Board to issue regulations to create additional exceptions that are determined to be necessary and appropriate to permit the sharing of medical information among affiliates. The Board is adopting the interim final rule to create exceptions that permit creditors to obtain and use medical information in credit eligibility determinations, restate the limits on redisclosure, and restate and add to the exceptions that allow sharing among affiliates. The **SUPPLEMENTARY INFORMATION** above contains information on the objectives of the interim final rule.

2. *Summary of issues raised by comments in response to the initial regulatory flexibility analysis.* In accordance with section 3(a) of the Regulatory Flexibility Act, the Board conducted an initial regulatory flexibility analysis in connection with the proposed rule. The Board did not receive any comments on its initial regulatory flexibility analysis.

3. *Description of small entities affected by the proposal.* Each section of the interim final rule applies to different types of small entities and specifies the types of small entities subject to that section. The interim final rule would apply, in whole or in part, to banks that are members of the Federal Reserve System (other than national banks) and their subsidiaries, branches and Agencies of foreign banks (other than Federal branches, Federal Agencies, and insured State branches of foreign banks) and their subsidiaries, commercial lending companies owned or controlled by foreign banks, organizations operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601 *et seq.*, and 611 *et seq.*), bank holding companies and affiliates of such holding companies (other than depository institutions and consumer reporting agencies), and creditors that participate in a transaction with one of the above-mentioned entities. A separate rule would apply to creditors not otherwise subject to one of the Agency rules. The Board's interim final rule will apply to the following institutions (numbers approximate): State member banks (932), bank holding companies (5,152), holding company non-bank subsidiaries (2,131), U.S. branches and agencies of foreign banks (289), and Edge and agreement corporations (75), for a subtotal of approximately 8,579 institutions. The Board estimates that over 5,000 of these institutions could be considered small institutions with assets less than $150 million. The Board is unable to estimate the number of creditors that may participate in transactions with such institutions or the number of other creditors that may be covered by the separate rule.

All small entities that are creditors will be affected by the provision of the interim final rule that addresses the prohibition on, and exceptions to, creditors obtaining or using medical information in connection with credit eligibility determinations. All small creditors will have to comply with the exceptions if they obtain or use medical information about consumers in connection with any credit eligibility determination.

4. *Recordkeeping, reporting, and compliance requirements.* The interim final rule requires certain documentation to qualify for some of the specific exceptions, as discussed in the **SUPPLEMENTARY INFORMATION** above. The interim final rule contains no reporting or disclosure requirements.

5. *Steps taken to minimize the economic impact on small entities.* The Board solicited comment on how to minimize the economic impact on small entities. The Board did not receive any comments on this issue. By adopting consistent rules and exceptions, the Board and the other Agencies have attempted to minimize the economic impact on small entities.

FDIC: The Agencies received no comments on their initial regulatory flexibility analyses. Upon further analysis, the FDIC certifies that this rule creating exceptions to the FACT Act's general prohibition on creditors obtaining or using medical information

pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit will not have a significant economic impact on small entities. This interim final rule, as authorized by section 411 of the FACT Act, creates exceptions to allow creditors to obtain or use medical information for eligibility purposes where necessary and appropriate to protect legitimate operational, transactional risk, consumer, and other needs, consistent with the Congressional intent to restrict the use of medical information for inappropriate purposes. The rule also excludes, in certain situations, medical information shared by a covered entity with an affiliate from the definition of a consumer report in section 603(d) of the FCRA, and addresses the reuse and redisclosure of medical information.

OTS: In accordance with section 603(a) of the Regulatory Flexibility Act (RFA) (5 U.S.C. 603(a)), OTS conducted an initial regulatory flexibility analysis in connection with the April 28, 2004 proposed rule. OTS did not receive any comments on its initial regulatory flexibility analysis.

Upon further analysis, OTS certifies in accordance with section 605(b) of the RFA (5 U.S.C. 605(b)) that this interim final rule will not have a significant economic impact on a substantial number of small entities. The Small Business Administration (SBA) has generally defined small savings institutions for RFA purposes as those with assets of $150 million or less. 13 CFR 121.201.

This interim final rule implements section 411 of the FACT Act and imposes only minimal economic impact. Section 571.30 creates exceptions to allow creditors to obtain or use medical information for credit eligibility purposes where necessary and appropriate to protect legitimate operational, transactional risk, consumer, and other needs, consistent with the congressional intent to restrict the use of medical information for inappropriate purposes. It applies to all any of the following, regardless of size, that participates as a creditor in a transaction: (1) A savings association; (2) a subsidiary owned in whole or in part by a savings association; (3) a savings and loan holding company; (4) a subsidiary of a savings and loan holding company other than a bank or subsidiary of a bank; (5) a service corporation owned in whole or in part by a savings association; or (6) any other person that participates as a creditor in a transaction involving a person described (1)–(5).

Section 571.31 implements the FACT Act's restrictions on the redisclosure of information. Section 571.32 implements the FACT Act's restrictions on the sharing of medical information among affiliates and includes exceptions to permit the sharing of medical information in certain circumstances. These sections apply to savings associations and Federal savings association operating subsidiaries, regardless of size.

As referenced elsewhere in this **SUPPLEMENTARY INFORMATION,** other laws and regulations, such as the Fair Housing Act, the Americans with Disabilities Act, and OTS's anti-discrimination rules in 12 CFR part 528, also limit or regulate obtaining and using medical information for credit eligibility determinations in a manner that discriminates against persons whose medical condition constitutes a ''disability'' or ''handicap'' under those authorities. Other laws, such as the GLB Act, HIPAA, and other parts of the FCRA, also limit or regulate the use, collection, and sharing of consumer information, including medical information. The industry's preexisting familiarity and compliance with the requirements of these other authorities to the extent applicable is one factor that OTS expects will minimize the economic impact of today's interim final rule.

NCUA: The Regulatory Flexibility Act requires NCUA to prepare an analysis to describe any significant economic impact any regulation may have on a substantial number of small entities. NCUA considers credit unions having less than ten million dollars in assets to be small for purposes of the Regulatory Flexibility Act. NCUA Interpretive Ruling and Policy Statement (IRPS) 87–2, as amended by IRPS 03–2. NCUA conducted an initial regulatory flexibility analysis in connection with the proposed rule and did not receive any comments on it.

Upon further review, NCUA certifies that this interim final rule will not have a significant economic impact on a substantial number of small entities. The interim final rule applies to all Federal credit unions that obtain or use a consumer's medical information in connection with credit determinations, regardless of credit union size. The interim final rule creates exceptions to the FACT Act's prohibition against Federal credit unions obtaining and using such information in connection with credit determinations. Additionally, the interim final rule implements the FACT Act's restrictions on the sharing of medical information among Federal credit union affiliates, credit union service organizations (CUSOs), and includes exceptions to permit the sharing of medical information in certain circumstances.

FDIC—Small Business Regulatory Enforcement Act

The Small Business Regulatory Enforcement Act of 1996 (SBREFA) (Pub. L. 104–121, 110 Stat. 857) provides generally for agencies to report rules to Congress and for Congress to review these rules. The reporting requirement is triggered in instances where the FDIC issues a final rule as defined by the Administrative Procedure Act (APA) (5 U.S.C. 55, *et seq.*). Because the FDIC is issuing a final rule as defined by the APA, the FDIC will file the reports required by SBREFA.

OCC and OTS Executive Order 12866 Determination

The OCC and OTS each has determined that its portion of the rule is not a significant regulatory action under Executive Order 12866.

OCC Executive Order 13132 Determination

The OCC has determined that this rule does not have any Federalism implications, as required by Executive Order 13132.

NCUA Executive Order 13132 Determination

Executive Order 13132 encourages independent regulatory agencies to consider the impact of their actions on state and local interests. In adherence to fundamental federalism principles, the NCUA, an independent regulatory agency as defined in 44 U.S.C. 3502(5), voluntarily complies with the executive order. The rule applies only to federally chartered credit unions and would not have substantial direct effects on the states, on the connection between the national government and the states, or on the distribution of power and responsibilities among the various levels of government. The NCUA has determined that this rule does not constitute a policy that has federalism implications for purposes of the executive order.

OCC and OTS Unfunded Mandates Reform Act of 1995 Determination

Section 202 of the Unfunded Mandates Reform Act of 1995, Public Law 104–4 (Unfunded Mandates Act) requires that an agency prepare a budgetary impact statement before promulgating a rule that includes a Federal mandate that may result in expenditure by State, local, and tribal

governments, in the aggregate, or by the private sector, of $100 million or more in any one year. If a budgetary impact statement is required, section 205 of the Unfunded Mandates Act also requires an agency to identify and consider a reasonable number of regulatory alternatives before promulgating a rule. The OCC and OTS each has determined that this rule will not result in expenditures by State, local, and tribal governments, or by the private sector, of $100 million or more. Accordingly, neither the OCC nor the OTS has prepared a budgetary impact statement or specifically addressed the regulatory alternatives considered.

NCUA: The Treasury and General Government Appropriations Act, 1999—Assessment of Federal Regulations and Policies on Families

The NCUA has determined that this rule would not affect family well-being within the meaning of section 654 of the Treasury and General Government Appropriations Act, 1999, Pub. L. 105–277, 112 Stat. 2681 (1998).

Plain Language Requirement

Section 722 of the Gramm-Leach-Bliley Act (GLBA) (12 U.S.C. 4809), requires the Federal banking agencies to use plain language in all proposed and final rules published after January 1, 2000. The proposed rule requested comments on how the rule might be changed to reflect the requirements of GLBA. No GLBA comments were received.

List of Subjects

12 CFR Part 41

Banks, banking, Consumer protection, National banks, Reporting and recordkeeping requirements.

12 CFR Part 222

Banks, banking, Consumer protection, Credit, Fair Credit Reporting Act, Holding companies, Privacy, Reporting and recordkeeping requirements, State member banks.

12 CFR Part 232

Consumer protection, Credit, Fair Credit Reporting Act, Privacy, Reporting and recordkeeping requirements.

12 CFR Part 334

Administrative practice and procedure, Bank deposit insurance, Banks, banking, Reporting and recordkeeping requirements, Safety and soundness.

12 CFR Part 571

Consumer protection, Credit, Fair Credit Reporting Act, Privacy, Reporting and recordkeeping requirements, Savings associations.

12 CFR Part 717

Consumer protection, Credit unions, Fair credit reporting, Medical information, Privacy, Reporting and recordkeeping requirements.

Office of the Comptroller of the Currency

12 CFR Chapter I.

Authority and Issuance

■ For the reasons set forth in the preamble, the OCC amends Chapter I of Title 12 of the Code of Federal Regulations as follows:

PART 41—FAIR CREDIT

■ 1. Revise the authority citation for part 41 to read as follows:

Authority: 12 U.S.C. 1 *et seq.*, 24(Seventh), 93a, 481, 484, and 1818; 15 U.S.C. 1681a, 1681b, 1681s, 1681w, 6801, and 6805.

■ 2. Revise subpart A to read as follows:

Subpart A—General Provisions

§ 41.2 Examples.

The examples in this part are not exclusive. Compliance with an example, to the extent applicable, constitutes compliance with this part. Examples in a paragraph illustrate only the issue described in the paragraph and do not illustrate any other issue that may arise in this part.

§ 41.3 Definitions.

As used in this part, unless the context requires otherwise:

(a) *Act* means the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*).

(b) *Affiliate* means any company that is related by common ownership or common corporate control with another company.

(c) [Reserved]

(d) *Company* means any corporation, limited liability company, business trust, general or limited partnership, association, or similar organization.

(e) *Consumer* means an individual.

(f) [Reserved]

(g) [Reserved]

(h) [Reserved]

(i) *Common ownership or common corporate control* means a relationship between two companies under which:

(1) One company has, with respect to the other company:

(i) Ownership, control, or power to vote 25 percent or more of the outstanding shares of any class of voting security of a company, directly or indirectly, or acting through one or more other persons;

(ii) Control in any manner over the election of a majority of the directors, trustees, or general partners (or individuals exercising similar functions) of a company; or

(iii) The power to exercise, directly or indirectly, a controlling influence over the management or policies of a company, as the OCC determines; or

(2) Any other person has, with respect to both companies, a relationship described in paragraphs (i)(1)(i)-(i)(1)(iii) of this section.

(j) [Reserved]

(k) *Medical information* means:

(1) Information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to—

(i) The past, present, or future physical, mental, or behavioral health or condition of an individual;

(ii) The provision of health care to an individual; or

(iii) The payment for the provision of health care to an individual.

(2) The term does not include:

(i) The age or gender of a consumer;

(ii) Demographic information about the consumer, including a consumer's residence address or e-mail address;

(iii) Any other information about a consumer that does not relate to the physical, mental, or behavioral health or condition of a consumer, including the existence or value of any insurance policy; or

(iv) Information that does not identify a specific consumer.

(l) *Person* means any individual, partnership, corporation, trust, estate cooperative, association, government or governmental subdivision or agency, or other entity.

■ 3. Add subpart D to read as follows:

Subpart D—Medical Information

§ 41.30 Obtaining or using medical information in connection with a determination of eligibility for credit.

(a) *Scope.* This section applies to:

(1) Any person that participates as a creditor in a transaction and that is a national bank, a Federal branch or agency of a foreign bank, and their respective subsidiaries; or

(2) Any other person that participates as a creditor in a transaction involving a person described in paragraph (a)(1) of this section.

(b) *General prohibition on obtaining or using medical information.* (1) *In general.* A creditor may not obtain or use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for

credit, except as provided in this section.

(2) *Definitions.* (i) *Credit* has the same meaning as in section 702 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a.

(ii) *Creditor* has the same meaning as in section 702 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a.

(iii) *Eligibility, or continued eligibility, for credit* means the consumer's qualification or fitness to receive, or continue to receive, credit, including the terms on which credit is offered. The term does not include:

(A) Any determination of the consumer's qualification or fitness for employment, insurance (other than a credit insurance product), or other non-credit products or services;

(B) Authorizing, processing, or documenting a payment or transaction on behalf of the consumer in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit; or

(C) Maintaining or servicing the consumer's account in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit.

(c) *Rule of construction for obtaining and using unsolicited medical information.* (1) *In general.* A creditor does not obtain medical information in violation of the prohibition if it receives medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit without specifically requesting medical information.

(2) *Use of unsolicited medical information.* A creditor that receives unsolicited medical information in the manner described in paragraph (c)(1) of this section may use that information in connection with any determination of the consumer's eligibility, or continued eligibility, for credit to the extent the creditor can rely on at least one of the exceptions in § 41.30(d) or (e).

(3) *Examples.* A creditor does not obtain medical information in violation of the prohibition if, for example:

(i) In response to a general question regarding a consumer's debts or expenses, the creditor receives information that the consumer owes a debt to a hospital.

(ii) In a conversation with the creditor's loan officer, the consumer informs the creditor that the consumer has a particular medical condition.

(iii) In connection with a consumer's application for an extension of credit, the creditor requests a consumer report from a consumer reporting agency and receives medical information in the consumer report furnished by the agency even though the creditor did not specifically request medical information from the consumer reporting agency.

(d) *Financial information exception for obtaining and using medical information.* (1) *In general.* A creditor may obtain and use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit so long as:

(i) The information is the type of information routinely used in making credit eligibility determinations, such as information relating to debts, expenses, income, benefits, assets, collateral, or the purpose of the loan, including the use of proceeds;

(ii) The creditor uses the medical information in a manner and to an extent that is no less favorable than it would use comparable information that is not medical information in a credit transaction; and

(iii) The creditor does not take the consumer's physical, mental, or behavioral health, condition or history, type of treatment, or prognosis into account as part of any such determination.

(2) *Examples.* (i) *Examples of the types of information routinely used in making credit eligibility determinations.* Paragraph (d)(1)(i) of this section permits a creditor, for example, to obtain and use information about:

(A) The dollar amount, repayment terms, repayment history, and similar information regarding medical debts to calculate, measure, or verify the repayment ability of the consumer, the use of proceeds, or the terms for granting credit;

(B) The value, condition, and lien status of a medical device that may serve as collateral to secure a loan;

(C) The dollar amount and continued eligibility for disability income or benefits related to health or a medical condition that is relied on as a source of repayment; or

(D) The identity of creditors to whom outstanding medical debts are owed in connection with an application for credit, including but not limited to, a transaction involving the consolidation of medical debts.

(ii) *Examples of uses of medical information consistent with the exception.* (A) A consumer includes on an application for credit information about two $20,000 debts. One debt is to a hospital; the other debt is to a retailer. The creditor contacts the hospital and the retailer to verify the amount and payment status of the debts. The creditor learns that both debts are more than 90 days past due. Any two debts of this size that are more than 90 days past due would disqualify the consumer under the creditor's established underwriting criteria. The creditor denies the application on the basis that the consumer has a poor repayment history on outstanding debts. The creditor has used medical information in a manner and to an extent no less favorable than it would use comparable non-medical information.

(B) A consumer indicates on an application for a $200,000 mortgage loan that she receives $15,000 in long-term disability income each year from her former employer and has no other income. Annual income of $15,000, regardless of source, would not be sufficient to support the requested amount of credit. The creditor denies the application on the basis that the projected debt-to-income ratio of the consumer does not meet the creditor's underwriting criteria. The creditor has used medical information in a manner and to an extent that is no less favorable than it would use comparable non-medical information.

(C) A consumer includes on an application for a $10,000 home equity loan that he has a $50,000 debt to a medical facility that specializes in treating a potentially terminal disease. The creditor contacts the medical facility to verify the debt and obtain the repayment history and current status of the loan. The creditor learns that the debt is current. The applicant meets the income and other requirements of the creditor's underwriting guidelines. The creditor grants the application. The creditor has used medical information in accordance with the exception.

(iii) *Examples of uses of medical information inconsistent with the exception.* (A) A consumer applies for $25,000 of credit and includes on the application information about a $50,000 debt to a hospital. The creditor contacts the hospital to verify the amount and payment status of the debt, and learns that the debt is current and that the consumer has no delinquencies in her repayment history. If the existing debt were instead owed to a retail department store, the creditor would approve the application and extend credit based on the amount and repayment history of the outstanding debt. The creditor, however, denies the application because the consumer is indebted to a hospital. The creditor has used medical information, here the identity of the medical creditor, in a manner and to an extent that is less favorable than it would use comparable non-medical information.

(B) A consumer meets with a loan officer of a creditor to apply for a

mortgage loan. While filling out the loan application, the consumer informs the loan officer orally that she has a potentially terminal disease. The consumer meets the creditor's established requirements for the requested mortgage loan. The loan officer recommends to the credit committee that the consumer be denied credit because the consumer has that disease. The credit committee follows the loan officer's recommendation and denies the application because the consumer has a potentially terminal disease. The creditor has used medical information in a manner inconsistent with the exception by taking into account the consumer's physical, mental, or behavioral health, condition, or history, type of treatment, or prognosis as part of a determination of eligibility or continued eligibility for credit.

(C) A consumer who has an apparent medical condition, such as a consumer who uses a wheelchair or an oxygen tank, meets with a loan officer to apply for a home equity loan. The consumer meets the creditor's established requirements for the requested home equity loan and the creditor typically does not require consumers to obtain a debt cancellation contract, debt suspension agreement, or credit insurance product in connection with such loans. However, based on the consumer's apparent medical condition, the loan officer recommends to the credit committee that credit be extended to the consumer only if the consumer obtains a debt cancellation contract, debt suspension agreement, or credit insurance product. The credit committee agrees with the loan officer's recommendation. The loan officer informs the consumer that the consumer must obtain a debt cancellation contract, debt suspension agreement, or credit insurance product to qualify for the loan. The consumer obtains one of these products from a third party and the creditor approves the loan. The creditor has used medical information in a manner inconsistent with the exception by taking into account the consumer's physical, mental, or behavioral health, condition, or history, type of treatment, or prognosis in setting conditions on the consumer's eligibility for credit.

(e) *Specific exceptions for obtaining and using medical information.* (1) *In general.* A creditor may obtain and use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit—

(i) To determine whether the use of a power of attorney or legal representative that is triggered by a medical event or condition is necessary and appropriate or whether the consumer has the legal capacity to contract when a person seeks to exercise a power of attorney or act as legal representative for a consumer based on an asserted medical event or condition;

(ii) To comply with applicable requirements of local, State, or Federal laws;

(iii) To determine, at the consumer's request, whether the consumer qualifies for a legally permissible special credit program or credit-related assistance program that is—

(A) Designed to meet the special needs of consumers with medical conditions; and

(B) Established and administered pursuant to a written plan that—

(*1*) Identifies the class of persons that the program is designed to benefit; and

(*2*) Sets forth the procedures and standards for extending credit or providing other credit-related assistance under the program.

(iv) To the extent necessary for purposes of fraud prevention or detection;

(v) In the case of credit for the purpose of financing medical products or services, to determine and verify the medical purpose of a loan and the use of proceeds;

(vi) Consistent with safe and sound practices, if the consumer or the consumer's legal representative specifically requests that the creditor use medical information in determining the consumer's eligibility, or continued eligibility, for credit, to accommodate the consumer's particular circumstances, and such request is documented by the creditor;

(vii) Consistent with safe and sound practices, to determine whether the provisions of a forbearance practice or program that is triggered by a medical event or condition apply to a consumer;

(viii) To determine the consumer's eligibility for, the triggering of, or the reactivation of a debt cancellation contract or debt suspension agreement if a medical condition or event is a triggering event for the provision of benefits under the contract or agreement; or

(ix) To determine the consumer's eligibility for, the triggering of, or the reactivation of a credit insurance product if a medical condition or event is a triggering event for the provision of benefits under the product.

(2) *Example of determining eligibility for a special credit program or credit assistance program.* A not-for-profit organization establishes a credit assistance program pursuant to a written plan that is designed to assist disabled veterans in purchasing homes by subsidizing the down payment for the home purchase mortgage loans of qualifying veterans. The organization works through mortgage lenders and requires mortgage lenders to obtain medical information about the disability of any consumer that seeks to qualify for the program, use that information to verify the consumer's eligibility for the program, and forward that information to the organization. A consumer who is a veteran applies to a creditor for a home purchase mortgage loan. The creditor informs the consumer about the credit assistance program for disabled veterans and the consumer seeks to qualify for the program. Assuming that the program complies with all applicable law, including applicable fair lending laws, the creditor may obtain and use medical information about the medical condition and disability, if any, of the consumer to determine whether the consumer qualifies for the credit assistance program.

(3) *Examples of verifying the medical purpose of the loan or the use of proceeds.* (i) If a consumer applies for $10,000 of credit for the purpose of financing vision correction surgery, the creditor may verify with the surgeon that the procedure will be performed. If the surgeon reports that surgery will not be performed on the consumer, the creditor may use that medical information to deny the consumer's application for credit, because the loan would not be used for the stated purpose.

(ii) If a consumer applies for $10,000 of credit for the purpose of financing cosmetic surgery, the creditor may confirm the cost of the procedure with the surgeon. If the surgeon reports that the cost of the procedure is $5,000, the creditor may use that medical information to offer the consumer only $5,000 of credit.

(iii) A creditor has an established medical loan program for financing particular elective surgical procedures. The creditor receives a loan application from a consumer requesting $10,000 of credit under the established loan program for an elective surgical procedure. The consumer indicates on the application that the purpose of the loan is to finance an elective surgical procedure not eligible for funding under the guidelines of the established loan program. The creditor may deny the consumer's application because the purpose of the loan is not for a particular procedure funded by the established loan program.

(4) *Examples of obtaining and using medical information at the request of*

the consumer. (i) If a consumer applies for a loan and specifically requests that the creditor consider the consumer's medical disability at the relevant time as an explanation for adverse payment history information in his credit report, the creditor may consider such medical information in evaluating the consumer's willingness and ability to repay the requested loan to accommodate the consumer's particular circumstances, consistent with safe and sound practices. The creditor may also decline to consider such medical information to accommodate the consumer, but may evaluate the consumer's application in accordance with its otherwise applicable underwriting criteria. The creditor may not deny the consumer's application or otherwise treat the consumer less favorably because the consumer specifically requested a medical accommodation, if the creditor would have extended the credit or treated the consumer more favorably under the creditor's otherwise applicable underwriting criteria.

(ii) If a consumer applies for a loan by telephone and explains that his income has been and will continue to be interrupted on account of a medical condition and that he expects to repay the loan by liquidating assets, the creditor may, but is not required to, evaluate the application using the sale of assets as the primary source of repayment, consistent with safe and sound practices, provided that the creditor documents the consumer's request by recording the oral conversation or making a notation of the request in the consumer's file.

(iii) If a consumer applies for a loan and the application form provides a space where the consumer may provide any other information or special circumstances, whether medical or non-medical, that the consumer would like the creditor to consider in evaluating the consumer's application, the creditor may use medical information provided by the consumer in that space on that application to accommodate the consumer's application for credit, consistent with safe and sound practices, or may disregard that information.

(iv) If a consumer specifically requests that the creditor use medical information in determining the consumer's eligibility, or continued eligibility, for credit and provides the creditor with medical information for that purpose, and the creditor determines that it needs additional information regarding the consumer's circumstances, the creditor may request, obtain, and use additional medical information about the consumer as necessary to verify the information provided by the consumer or to determine whether to make an accommodation for the consumer. The consumer may decline to provide additional information, withdraw the request for an accommodation, and have the application considered under the creditor's otherwise applicable underwriting criteria.

(v) If a consumer completes and signs a credit application that is not for medical purpose credit and the application contains boilerplate language that routinely requests medical information from the consumer or that indicates that by applying for credit the consumer authorizes or consents to the creditor obtaining and using medical information in connection with a determination of the consumer's eligibility, or continued eligibility, for credit, the consumer has not specifically requested that the creditor obtain and use medical information to accommodate the consumer's particular circumstances.

(5) *Example of a forbearance practice or program.* After an appropriate safety and soundness review, a creditor institutes a program that allows consumers who are or will be hospitalized to defer payments as needed for up to three months, without penalty, if the credit account has been open for more than one year and has not previously been in default, and the consumer provides confirming documentation at an appropriate time. A consumer is hospitalized and does not pay her bill for a particular month. This consumer has had a credit account with the creditor for more than one year and has not previously been in default. The creditor attempts to contact the consumer and speaks with the consumer's adult child, who is not the consumer's legal representative. The adult child informs the creditor that the consumer is hospitalized and is unable to pay the bill at that time. The creditor defers payments for up to three months, without penalty, for the hospitalized consumer and sends the consumer a letter confirming this practice and the date on which the next payment will be due.

§ 41.31 Limits on redisclosure of information.

(a) *Scope.* This section applies to national banks, Federal branches and agencies of foreign banks, and their respective operating subsidiaries.

(b) *Limits on redisclosure.* If a person described in paragraph (a) of this section receives medical information about a consumer from a consumer reporting agency or its affiliate, the person must not disclose that information to any other person, except as necessary to carry out the purpose for which the information was initially disclosed, or as otherwise permitted by statute, regulation, or order.

§ 41.32 Sharing medical information with affiliates.

(a) *Scope.* This section applies to national banks, Federal branches and agencies of foreign banks, and their respective operating subsidiaries.

(b) *In general.* The exclusions from the term ''consumer report'' in section 603(d)(2) of the Act that allow the sharing of information with affiliates do not apply if a person described in paragraph (a) of this section communicates to an affiliate—

(1) Medical information;

(2) An individualized list or description based on the payment transactions of the consumer for medical products or services; or

(3) An aggregate list of identified consumers based on payment transactions for medical products or services.

(c) *Exceptions.* A person described in paragraph (a) may rely on the exclusions from the term ''consumer report'' in section 603(d)(2) of the Act to communicate the information in paragraph (b) to an affiliate—

(1) In connection with the business of insurance or annuities (including the activities described in section 18B of the model Privacy of Consumer Financial and Health Information Regulation issued by the National Association of Insurance Commissioners, as in effect on January 1, 2003);

(2) For any purpose permitted without authorization under the regulations promulgated by the Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA);

(3) For any purpose referred to in section 1179 of HIPAA;

(4) For any purpose described in section 502(e) of the Gramm-Leach-Bliley Act;

(5) In connection with a determination of the consumer's eligibility, or continued eligibility, for credit consistent with § 41.30; or

(6) As otherwise permitted by order of the OCC.

Board of Governors of the Federal Reserve System

12 CFR Chapter II.

Authority and Issuance

■ For the reasons set forth in the joint preamble, title 12, chapter II, of the

Code
of Federal Regulations is amended as follows:

PART 222—FAIR CREDIT REPORTING (REGULATION V)

■ 1. The authority citation for part 222 is revised to read as follows:

Authority: 15 U.S.C. 1681b and 1681s; Secs. 3, 214, and 217, Pub. L. 108–159, 117 Stat. 1952.

Subpart A—General Provisions

■ 2. Amend subpart A to part 222 by adding §§ 222.2 and 222.3 to read as follows:

§ 222.2 Examples.

The examples in this part are not exclusive. Compliance with an example, to the extent applicable, constitutes compliance with this part. Examples in a paragraph illustrate only the issue described in the paragraph and do not illustrate any other issue that may arise in this part.

§ 222.3 Definitions.

As used in this part, unless the context requires otherwise:

(a) *Act* means the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*).

(b) *Affiliate* means any company that is related by common ownership or common corporate control with another company.

(c) [Reserved]

(d) *Company* means any corporation, limited liability company, business trust, general or limited partnership, association, or similar organization.

(e) *Consumer* means an individual.

(f) [Reserved]

(g) [Reserved]

(h) [Reserved]

(i) *Common ownership or common corporate control* means a relationship between two companies under which:

(1) One company has, with respect to the other company:

(i) Ownership, control, or power to vote 25 percent or more of the outstanding shares of any class of voting security of a company, directly or indirectly, or acting through one or more other persons;

(ii) Control in any manner over the election of a majority of the directors, trustees, or general partners (or individuals exercising similar functions) of a company; or

(iii) The power to exercise, directly or indirectly, a controlling influence over the management or policies of a company, as the Board determines; or

(2) Any other person has, with respect to both companies, a relationship described in paragraphs (i)(1)(i)–(i)(1)(iii) of this section.

(j) [Reserved]

(k) *Medical information* means:

(1) Information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to—

(i) The past, present, or future physical, mental, or behavioral health or condition of an individual;

(ii) The provision of health care to an individual; or

(iii) The payment for the provision of health care to an individual.

(2) The term does not include:

(i) The age or gender of a consumer;

(ii) Demographic information about the consumer, including a consumer's residence address or e-mail address;

(iii) Any other information about a consumer that does not relate to the physical, mental, or behavioral health or condition of a consumer, including the existence or value of any insurance policy; or

(iv) Information that does not identify a specific consumer.

(l) *Person* means any individual, partnership, corporation, trust, estate cooperative, association, government or governmental subdivision or agency, or other entity.

■ 3. Subpart D is added to part 222 to read as follows:

Subpart D—Medical Information

Sec.

Subpart D—Medical Information

§ 222.30 Obtaining or using medical information in connection with a determination of eligibility for credit.

(a) *Scope.* This section applies to

(1) Any of the following that participates as a creditor in a transaction—

(i) A bank that is a member of the Federal Reserve System (other than national banks) and its subsidiaries;

(ii) A branch or Agency of a foreign bank (other than Federal branches, Federal Agencies, and insured State branches of foreign banks) and its subsidiaries;

(iii) A commercial lending company owned or controlled by foreign banks;

(iv) An organization operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601 *et seq.*, and 611 *et seq.*);

(v) A bank holding company and an affiliate of such holding company (other than depository institutions and consumer reporting agencies); or

(2) Any other person that participates as a creditor in a transaction involving a person described in paragraph (a)(1) of this section.

(b) *General prohibition on obtaining or using medical information.* (1) *In general.* A creditor may not obtain or use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit, except as provided in this section.

(2) *Definitions.* (i) *Credit* has the same meaning as in section 702 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a.

(ii) *Creditor* has the same meaning as in section 702 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a.

(iii) *Eligibility, or continued eligibility, for credit* means the consumer's qualification or fitness to receive, or continue to receive, credit, including the terms on which credit is offered. The term does not include:

(A) Any determination of the consumer's qualification or fitness for employment, insurance (other than a credit insurance product), or other non-credit products or services;

(B) Authorizing, processing, or documenting a payment or transaction on behalf of the consumer in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit; or

(C) Maintaining or servicing the consumer's account in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit.

(c) *Rule of construction for obtaining and using unsolicited medical information.* (1) *In general.* A creditor does not obtain medical information in violation of the prohibition if it receives medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit without specifically requesting medical information.

(2) *Use of unsolicited medical information.* A creditor that receives unsolicited medical information in the manner described in paragraph (c)(1) of this section may use that information in connection with any determination of the consumer's eligibility, or continued eligibility, for credit to the extent the creditor can rely on at least one of the exceptions in § 222.30(d) or (e).

(3) *Examples.* A creditor does not obtain medical information in violation of the prohibition if, for example:

(i) In response to a general question regarding a consumer's debts or expenses, the creditor receives information that the consumer owes a debt to a hospital.

(ii) In a conversation with the creditor's loan officer, the consumer informs the creditor that the consumer has a particular medical condition.

(iii) In connection with a consumer's application for an extension of credit, the creditor requests a consumer report from a consumer reporting agency and receives medical information in the consumer report furnished by the agency even though the creditor did not specifically request medical information from the consumer reporting agency.

(d) *Financial information exception for obtaining and using medical information.* (1) *In general.* A creditor may obtain and use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit so long as:

(i) The information is the type of information routinely used in making credit eligibility determinations, such as information relating to debts, expenses, income, benefits, assets, collateral, or the purpose of the loan, including the use of proceeds;

(ii) The creditor uses the medical information in a manner and to an extent that is no less favorable than it would use comparable information that is not medical information in a credit transaction; and

(iii) The creditor does not take the consumer's physical, mental, or behavioral health, condition or history, type of treatment, or prognosis into account as part of any such determination.

(2) *Examples.* (i) *Examples of the types of information routinely used in making credit eligibility determinations.* Paragraph (d)(1)(i) of this section permits a creditor, for example, to obtain and use information about:

(A) The dollar amount, repayment terms, repayment history, and similar information regarding medical debts to calculate, measure, or verify the repayment ability of the consumer, the use of proceeds, or the terms for granting credit;

(B) The value, condition, and lien status of a medical device that may serve as collateral to secure a loan;

(C) The dollar amount and continued eligibility for disability income or benefits related to health or a medical condition that is relied on as a source of repayment; or

(D) The identity of creditors to whom outstanding medical debts are owed in connection with an application for credit, including but not limited to, a transaction involving the consolidation of medical debts.

(ii) *Examples of uses of medical information consistent with the exception.* (A) A consumer includes on an application for credit information about two $20,000 debts. One debt is to a hospital; the other debt is to a retailer. The creditor contacts the hospital and the retailer to verify the amount and payment status of the debts. The creditor learns that both debts are more than 90 days past due. Any two debts of this size that are more than 90 days past due would disqualify the consumer under the creditor's established underwriting criteria. The creditor denies the application on the basis that the consumer has a poor repayment history on outstanding debts. The creditor has used medical information in a manner and to an extent no less favorable than it would use comparable non-medical information.

(B) A consumer indicates on an application for a $200,000 mortgage loan that she receives $15,000 in long-term disability income each year from her former employer and has no other income. Annual income of $15,000, regardless of source, would not be sufficient to support the requested amount of credit. The creditor denies the application on the basis that the projected debt-to-income ratio of the consumer does not meet the creditor's underwriting criteria. The creditor has used medical information in a manner and to an extent that is no less favorable than it would use comparable non-medical information.

(C) A consumer includes on an application for a $10,000 home equity loan that he has a $50,000 debt to a medical facility that specializes in treating a potentially terminal disease. The creditor contacts the medical facility to verify the debt and obtain the repayment history and current status of the loan. The creditor learns that the debt is current. The applicant meets the income and other requirements of the creditor's underwriting guidelines. The creditor grants the application. The creditor has used medical information in accordance with the exception.

(iii) *Examples of uses of medical information inconsistent with the exception.* (A) A consumer applies for $25,000 of credit and includes on the application information about a $50,000 debt to a hospital. The creditor contacts the hospital to verify the amount and payment status of the debt, and learns that the debt is current and that the consumer has no delinquencies in her repayment history. If the existing debt were instead owed to a retail department store, the creditor would approve the application and extend credit based on the amount and repayment history of the outstanding debt. The creditor, however, denies the application because the consumer is indebted to a hospital. The creditor has used medical information, here the identity of the medical creditor, in a manner and to an extent that is less favorable than it would use comparable non-medical information.

(B) A consumer meets with a loan officer of a creditor to apply for a mortgage loan. While filling out the loan application, the consumer informs the loan officer orally that she has a potentially terminal disease. The consumer meets the creditor's established requirements for the requested mortgage loan. The loan officer recommends to the credit committee that the consumer be denied credit because the consumer has that disease. The credit committee follows the loan officer's recommendation and denies the application because the consumer has a potentially terminal disease. The creditor has used medical information in a manner inconsistent with the exception by taking into account the consumer's physical, mental, or behavioral health, condition, or history, type of treatment, or prognosis as part of a determination of eligibility or continued eligibility for credit.

(C) A consumer who has an apparent medical condition, such as a consumer who uses a wheelchair or an oxygen tank, meets with a loan officer to apply for a home equity loan. The consumer meets the creditor's established requirements for the requested home equity loan and the creditor typically does not require consumers to obtain a debt cancellation contract, debt suspension agreement, or credit insurance product in connection with such loans. However, based on the consumer's apparent medical condition, the loan officer recommends to the credit committee that credit be extended to the consumer only if the consumer obtains a debt cancellation contract, debt suspension agreement, or credit insurance product. The credit committee agrees with the loan officer's recommendation. The loan officer informs the consumer that the consumer must obtain a debt cancellation contract, debt suspension agreement, or credit insurance product to qualify for the loan. The consumer obtains one of these products from a third party and the creditor approves the loan. The creditor has used medical information in a manner inconsistent with the exception by taking into account the consumer's

physical, mental, or behavioral health, condition, or history, type of treatment, or prognosis in setting conditions on the consumer's eligibility for credit.

(e) *Specific exceptions for obtaining and using medical information.* (1) *In general.* A creditor may obtain and use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit—

(i) To determine whether the use of a power of attorney or legal representative that is triggered by a medical event or condition is necessary and appropriate or whether the consumer has the legal capacity to contract when a person seeks to exercise a power of attorney or act as legal representative for a consumer based on an asserted medical event or condition;

(ii) To comply with applicable requirements of local, State, or Federal laws;

(iii) To determine, at the consumer's request, whether the consumer qualifies for a legally permissible special credit program or credit-related assistance program that is—

(A) Designed to meet the special needs of consumers with medical conditions; and

(B) Established and administered pursuant to a written plan that—

(*1*) Identifies the class of persons that the program is designed to benefit; and

(*2*) Sets forth the procedures and standards for extending credit or providing other credit-related assistance under the program.

(iv) To the extent necessary for purposes of fraud prevention or detection;

(v) In the case of credit for the purpose of financing medical products or services, to determine and verify the medical purpose of a loan and the use of proceeds;

(vi) Consistent with safe and sound practices, if the consumer or the consumer's legal representative specifically requests that the creditor use medical information in determining the consumer's eligibility, or continued eligibility, for credit, to accommodate the consumer's particular circumstances, and such request is documented by the creditor;

(vii) Consistent with safe and sound practices, to determine whether the provisions of a forbearance practice or program that is triggered by a medical event or condition apply to a consumer;

(viii) To determine the consumer's eligibility for, the triggering of, or the reactivation of a debt cancellation contract or debt suspension agreement if a medical condition or event is a triggering event for the provision of benefits under the contract or agreement; or

(ix) To determine the consumer's eligibility for, the triggering of, or the reactivation of a credit insurance product if a medical condition or event is a triggering event for the provision of benefits under the product.

(2) *Example of determining eligibility for a special credit program or credit assistance program.* A not-for-profit organization establishes a credit assistance program pursuant to a written plan that is designed to assist disabled veterans in purchasing homes by subsidizing the down payment for the home purchase mortgage loans of qualifying veterans. The organization works through mortgage lenders and requires mortgage lenders to obtain medical information about the disability of any consumer that seeks to qualify for the program, use that information to verify the consumer's eligibility for the program, and forward that information to the organization. A consumer who is a veteran applies to a creditor for a home purchase mortgage loan. The creditor informs the consumer about the credit assistance program for disabled veterans and the consumer seeks to qualify for the program. Assuming that the program complies with all applicable law, including applicable fair lending laws, the creditor may obtain and use medical information about the medical condition and disability, if any, of the consumer to determine whether the consumer qualifies for the credit assistance program.

(3) *Examples of verifying the medical purpose of the loan or the use of proceeds.* (i) If a consumer applies for $10,000 of credit for the purpose of financing vision correction surgery, the creditor may verify with the surgeon that the procedure will be performed. If the surgeon reports that surgery will not be performed on the consumer, the creditor may use that medical information to deny the consumer's application for credit, because the loan would not be used for the stated purpose.

(ii) If a consumer applies for $10,000 of credit for the purpose of financing cosmetic surgery, the creditor may confirm the cost of the procedure with the surgeon. If the surgeon reports that the cost of the procedure is $5,000, the creditor may use that medical information to offer the consumer only $5,000 of credit.

(iii) A creditor has an established medical loan program for financing particular elective surgical procedures. The creditor receives a loan application from a consumer requesting $10,000 of credit under the established loan program for an elective surgical procedure. The consumer indicates on the application that the purpose of the loan is to finance an elective surgical procedure not eligible for funding under the guidelines of the established loan program. The creditor may deny the consumer's application because the purpose of the loan is not for a particular procedure funded by the established loan program.

(4) *Examples of obtaining and using medical information at the request of the consumer.* (i) If a consumer applies for a loan and specifically requests that the creditor consider the consumer's medical disability at the relevant time as an explanation for adverse payment history information in his credit report, the creditor may consider such medical information in evaluating the consumer's willingness and ability to repay the requested loan to accommodate the consumer's particular circumstances, consistent with safe and sound practices. The creditor may also decline to consider such medical information to accommodate the consumer, but may evaluate the consumer's application in accordance with its otherwise applicable underwriting criteria. The creditor may not deny the consumer's application or otherwise treat the consumer less favorably because the consumer specifically requested a medical accommodation, if the creditor would have extended the credit or treated the consumer more favorably under the creditor's otherwise applicable underwriting criteria.

(ii) If a consumer applies for a loan by telephone and explains that his income has been and will continue to be interrupted on account of a medical condition and that he expects to repay the loan by liquidating assets, the creditor may, but is not required to, evaluate the application using the sale of assets as the primary source of repayment, consistent with safe and sound practices, provided that the creditor documents the consumer's request by recording the oral conversation or making a notation of the request in the consumer's file.

(iii) If a consumer applies for a loan and the application form provides a space where the consumer may provide any other information or special circumstances, whether medical or non-medical, that the consumer would like the creditor to consider in evaluating the consumer's application, the creditor may use medical information provided by the consumer in that space on that application to accommodate the consumer's application for credit,

consistent with safe and sound practices, or may disregard that information.

(iv) If a consumer specifically requests that the creditor use medical information in determining the consumer's eligibility, or continued eligibility, for credit and provides the creditor with medical information for that purpose, and the creditor determines that it needs additional information regarding the consumer's circumstances, the creditor may request, obtain, and use additional medical information about the consumer as necessary to verify the information provided by the consumer or to determine whether to make an accommodation for the consumer. The consumer may decline to provide additional information, withdraw the request for an accommodation, and have the application considered under the creditor's otherwise applicable underwriting criteria.

(v) If a consumer completes and signs a credit application that is not for medical purpose credit and the application contains boilerplate language that routinely requests medical information from the consumer or that indicates that by applying for credit the consumer authorizes or consents to the creditor obtaining and using medical information in connection with a determination of the consumer's eligibility, or continued eligibility, for credit, the consumer has not specifically requested that the creditor obtain and use medical information to accommodate the consumer's particular circumstances.

(5) *Example of a forbearance practice or program.* After an appropriate safety and soundness review, a creditor institutes a program that allows consumers who are or will be hospitalized to defer payments as needed for up to three months, without penalty, if the credit account has been open for more than one year and has not previously been in default, and the consumer provides confirming documentation at an appropriate time. A consumer is hospitalized and does not pay her bill for a particular month. This consumer has had a credit account with the creditor for more than one year and has not previously been in default. The creditor attempts to contact the consumer and speaks with the consumer's adult child, who is not the consumer's legal representative. The adult child informs the creditor that the consumer is hospitalized and is unable to pay the bill at that time. The creditor defers payments for up to three months, without penalty, for the hospitalized consumer and sends the consumer a letter confirming this practice and the date on which the next payment will be due.

§ 222.31 Limits on redisclosure of information.

(a) *Scope.* This section applies to banks that are members of the Federal Reserve System (other than national banks) and their respective operating subsidiaries, branches and agencies of foreign banks (other than Federal branches, Federal Agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, organizations operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601 *et seq.*, and 611 *et seq.*), and bank holding companies and affiliates of such holding companies (other than depository institutions and consumer reporting agencies).

(b) *Limits on redisclosure.* If a person described in paragraph (a) of this section receives medical information about a consumer from a consumer reporting agency or its affiliate, the person must not disclose that information to any other person, except as necessary to carry out the purpose for which the information was initially disclosed, or as otherwise permitted by statute, regulation, or order.

§ 222.32 Sharing medical information with affiliates.

(a) *Scope.* This section applies to banks that are members of the Federal Reserve System (other than national banks) and their respective operating subsidiaries, branches and agencies of foreign banks (other than Federal branches, Federal Agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, organizations operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601 *et seq.*, and 611 *et seq.*).

(b) *In general.* The exclusions from the term ''consumer report'' in section 603(d)(2) of the Act that allow the sharing of information with affiliates do not apply to a person described in paragraph (a) of this section if that person communicates to an affiliate—

(1) Medical information;

(2) An individualized list or description based on the payment transactions of the consumer for medical products or services; or

(3) An aggregate list of identified consumers based on payment transactions for medical products or services.

(c) Exceptions. A person described in paragraph (a) of this section may rely on the exclusions from the term ''consumer report'' in section 603(d)(2) of the Act to communicate the information in paragraph (b) of this section to an affiliate—

(1) In connection with the business of insurance or annuities (including the activities described in section 18B of the model Privacy of Consumer Financial and Health Information Regulation issued by the National Association of Insurance Commissioners, as in effect on January 1, 2003);

(2) For any purpose permitted without authorization under the regulations promulgated by the Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA);

(3) For any purpose referred to in section 1179 of HIPAA;

(4) For any purpose described in section 502(e) of the Gramm-Leach-Bliley Act;

(5) In connection with a determination of the consumer's eligibility, or continued eligibility, for credit consistent with § 222.30 of this part; or

(6) As otherwise permitted by order of the Board.

■ 4. A new part 232 is added to read as follows:

PART 232—OBTAINING AND USING MEDICAL INFORMATION IN CONNECTION WITH CREDIT (REGULATION FF)

Sec.

Authority: 15 U.S.C. 1681b.

§ 232.1 Scope, general prohibition and definitions.

(a) *Scope.* This part applies to creditors, as defined in paragraph (c)(3) of this section, except for creditors that are subject to §§ 41.30, 222.30, 334.30, 571.30, or 717.30.

(b) *In general.* A creditor may not obtain or use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit, except as provided in this section.

(c) *Definitions.* (1) *Consumer* means an individual.

(2) *Credit* has the same meaning as in section 702 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a.

(3) *Creditor* has the same meaning as in section 702 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a.

(4) *Eligibility, or continued eligibility, for credit* means the consumer's qualification or fitness to receive, or continue to receive, credit, including the terms on which credit is offered. The term does not include:

(i) Any determination of the consumer's qualification or fitness for employment, insurance (other than a credit insurance product), or other non-credit products or services;

(ii) Authorizing, processing, or documenting a payment or transaction on behalf of the consumer in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit; or

(iii) Maintaining or servicing the consumer's account in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit.

(5) *Medical information* means:

(i) Information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to—

(A) The past, present, or future physical, mental, or behavioral health or condition of an individual;

(B) The provision of health care to an individual; or

(C) The payment for the provision of health care to an individual.

(ii) The term does not include:

(A) The age or gender of a consumer;

(B) Demographic information about the consumer, including a consumer's residence address or e-mail address;

(C) Any other information about a consumer that does not relate to the physical, mental, or behavioral health or condition of a consumer, including the existence or value of any insurance policy; or

(D) Information that does not identify a specific consumer.

(6) *Person* means any individual, partnership, corporation, trust, estate cooperative, association, government or governmental subdivision or agency, or other entity.

§ 232.2 Rule of construction for obtaining and using unsolicited medical information.

(a) *In general.* A creditor does not obtain medical information in violation of the prohibition if it receives medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit without specifically requesting medical information.

(b) *Use of unsolicited medical information.* A creditor that receives unsolicited medical information in the manner described in paragraph (a) of this section may use that information in connection with any determination of the consumer's eligibility, or continued eligibility, for credit to the extent the creditor can rely on at least one of the exceptions in § 232.3 or § 232.4.

(c) *Examples.* A creditor does not obtain medical information in violation of the prohibition if, for example:

(1) In response to a general question regarding a consumer's debts or expenses, the creditor receives information that the consumer owes a debt to a hospital.

(2) In a conversation with the creditor's loan officer, the consumer informs the creditor that the consumer has a particular medical condition.

(3) In connection with a consumer's application for an extension of credit, the creditor requests a consumer report from a consumer reporting agency and receives medical information in the consumer report furnished by the agency even though the creditor did not specifically request medical information from the consumer reporting agency.

§ 232.3 Financial information exception for obtaining and using medical information.

(a) *In general.* A creditor may obtain and use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit so long as:

(1) The information is the type of information routinely used in making credit eligibility determinations, such as information relating to debts, expenses, income, benefits, assets, collateral, or the purpose of the loan, including the use of proceeds;

(2) The creditor uses the medical information in a manner and to an extent that is no less favorable than it would use comparable information that is not medical information in a credit transaction; and

(3) The creditor does not take the consumer's physical, mental, or behavioral health, condition or history, type of treatment, or prognosis into account as part of any such determination.

(b) *Examples.* (1) *Examples of the types of information routinely used in making credit eligibility determinations.* Paragraph (a)(1) of this section permits a creditor, for example, to obtain and use information about:

(i) The dollar amount, repayment terms, repayment history, and similar information regarding medical debts to calculate, measure, or verify the repayment ability of the consumer, the use of proceeds, or the terms for granting credit;

(ii) The value, condition, and lien status of a medical device that may serve as collateral to secure a loan;

(iii) The dollar amount and continued eligibility for disability income or benefits related to health or a medical condition that is relied on as a source of repayment; or

(iv) The identity of creditors to whom outstanding medical debts are owed in connection with an application for credit, including but not limited to, a transaction involving the consolidation of medical debts.

(2) *Examples of uses of medical information consistent with the exception.* (i) A consumer includes on an application for credit information about two $20,000 debts. One debt is to a hospital; the other debt is to a retailer. The creditor contacts the hospital and the retailer to verify the amount and payment status of the debts. The creditor learns that both debts are more than 90 days past due. Any two debts of this size that are more than 90 days past due would disqualify the consumer under the creditor's established underwriting criteria. The creditor denies the application on the basis that the consumer has a poor repayment history on outstanding debts. The creditor has used medical information in a manner and to an extent no less favorable than it would use comparable non-medical information.

(ii) A consumer indicates on an application for a $200,000 mortgage loan that she receives $15,000 in long-term disability income each year from her former employer and has no other income. Annual income of $15,000, regardless of source, would not be sufficient to support the requested amount of credit. The creditor denies the application on the basis that the projected debt-to-income ratio of the consumer does not meet the creditor's underwriting criteria. The creditor has used medical information in a manner and to an extent that is no less favorable than it would use comparable non-medical information.

(iii) A consumer includes on an application for a $10,000 home equity loan that he has a $50,000 debt to a medical facility that specializes in treating a potentially terminal disease. The creditor contacts the medical facility to verify the debt and obtain the repayment history and current status of the loan. The creditor learns that the debt is current. The applicant meets the income and other requirements of the creditor's underwriting guidelines. The creditor grants the application. The

creditor has used medical information in accordance with the exception.

(3) *Examples of uses of medical information inconsistent with the exception.* (i) A consumer applies for $25,000 of credit and includes on the application information about a $50,000 debt to a hospital. The creditor contacts the hospital to verify the amount and payment status of the debt, and learns that the debt is current and that the consumer has no delinquencies in her repayment history. If the existing debt were instead owed to a retail department store, the creditor would approve the application and extend credit based on the amount and repayment history of the outstanding debt. The creditor, however, denies the application because the consumer is indebted to a hospital. The creditor has used medical information, here the identity of the medical creditor, in a manner and to an extent that is less favorable than it would use comparable non-medical information.

(ii) A consumer meets with a loan officer of a creditor to apply for a mortgage loan. While filling out the loan application, the consumer informs the loan officer orally that she has a potentially terminal disease. The consumer meets the creditor's established requirements for the requested mortgage loan. The loan officer recommends to the credit committee that the consumer be denied credit because the consumer has that disease. The credit committee follows the loan officer's recommendation and denies the application because the consumer has a potentially terminal disease. The creditor has used medical information in a manner inconsistent with the exception by taking into account the consumer's physical, mental, or behavioral health, condition, or history, type of treatment, or prognosis as part of a determination of eligibility or continued eligibility for credit.

(iii) A consumer who has an apparent medical condition, such as a consumer who uses a wheelchair or an oxygen tank, meets with a loan officer to apply for a home equity loan. The consumer meets the creditor's established requirements for the requested home equity loan and the creditor typically does not require consumers to obtain a debt cancellation contract, debt suspension agreement, or credit insurance product in connection with such loans. However, based on the consumer's apparent medical condition, the loan officer recommends to the credit committee that credit be extended to the consumer only if the consumer obtains a debt cancellation contract, debt suspension agreement, or credit insurance product. The credit committee agrees with the loan officer's recommendation. The loan officer informs the consumer that the consumer must obtain a debt cancellation contract, debt suspension agreement, or credit insurance product to qualify for the loan. The consumer obtains one of these products from a third party and the creditor approves the loan. The creditor has used medical information in a manner inconsistent with the exception by taking into account the consumer's physical, mental, or behavioral health, condition, or history, type of treatment, or prognosis in setting conditions on the consumer's eligibility for credit.

§ 232.4 Specific exceptions for obtaining and using medical information.

(a) *In general.* A creditor may obtain and use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit—

(1) To determine whether the use of a power of attorney or legal representative that is triggered by a medical event or condition is necessary and appropriate or whether the consumer has the legal capacity to contract when a person seeks to exercise a power of attorney or act as legal representative for a consumer based on an asserted medical event or condition;

(2) To comply with applicable requirements of local, State, or Federal laws;

(3) To determine, at the consumer's request, whether the consumer qualifies for a legally permissible special credit program or credit-related assistance program that is—

(i) Designed to meet the special needs of consumers with medical conditions; and

(ii) Established and administered pursuant to a written plan that—

(A) Identifies the class of persons that the program is designed to benefit; and

(B) Sets forth the procedures and standards for extending credit or providing other credit-related assistance under the program.

(4) To the extent necessary for purposes of fraud prevention or detection;

(5) In the case of credit for the purpose of financing medical products or services, to determine and verify the medical purpose of a loan and the use of proceeds;

(6) Consistent with safe and sound practices, if the consumer or the consumer's legal representative specifically requests that the creditor use medical information in determining the consumer's eligibility, or continued eligibility, for credit, to accommodate the consumer's particular circumstances, and such request is documented by the creditor;

(7) Consistent with safe and sound practices, to determine whether the provisions of a forbearance practice or program that is triggered by a medical event or condition apply to a consumer;

(8) To determine the consumer's eligibility for, the triggering of, or the reactivation of a debt cancellation contract or debt suspension agreement if a medical condition or event is a triggering event for the provision of benefits under the contract or agreement; or

(9) To determine the consumer's eligibility for, the triggering of, or the reactivation of a credit insurance product if a medical condition or event is a triggering event for the provision of benefits under the product.

(b) *Example of determining eligibility for a special credit program or credit assistance program.* A not-for-profit organization establishes a credit assistance program pursuant to a written plan that is designed to assist disabled veterans in purchasing homes by subsidizing the down payment for the home purchase mortgage loans of qualifying veterans. The organization works through mortgage lenders and requires mortgage lenders to obtain medical information about the disability of any consumer that seeks to qualify for the program, use that information to verify the consumer's eligibility for the program, and forward that information to the organization. A consumer who is a veteran applies to a creditor for a home purchase mortgage loan. The creditor informs the consumer about the credit assistance program for disabled veterans and the consumer seeks to qualify for the program. Assuming that the program complies with all applicable law, including applicable fair lending laws, the creditor may obtain and use medical information about the medical condition and disability, if any, of the consumer to determine whether the consumer qualifies for the credit assistance program.

(c) *Examples of verifying the medical purpose of the loan or the use of proceeds.* (1) If a consumer applies for $10,000 of credit for the purpose of financing vision correction surgery, the creditor may verify with the surgeon that the procedure will be performed. If the surgeon reports that surgery will not be performed on the consumer, the creditor may use that medical information to deny the consumer's application for credit, because the loan

would not be used for the stated purpose.

(2) If a consumer applies for $10,000 of credit for the purpose of financing cosmetic surgery, the creditor may confirm the cost of the procedure with the surgeon. If the surgeon reports that the cost of the procedure is $5,000, the creditor may use that medical information to offer the consumer only $5,000 of credit.

(3) A creditor has an established medical loan program for financing particular elective surgical procedures. The creditor receives a loan application from a consumer requesting $10,000 of credit under the established loan program for an elective surgical procedure. The consumer indicates on the application that the purpose of the loan is to finance an elective surgical procedure not eligible for funding under the guidelines of the established loan program. The creditor may deny the consumer's application because the purpose of the loan is not for a particular procedure funded by the established loan program.

(d) *Examples of obtaining and using medical information at the request of the consumer.* (1) If a consumer applies for a loan and specifically requests that the creditor consider the consumer's medical disability at the relevant time as an explanation for adverse payment history information in his credit report, the creditor may consider such medical information in evaluating the consumer's willingness and ability to repay the requested loan to accommodate the consumer's particular circumstances, consistent with safe and sound practices. The creditor may also decline to consider such medical information to accommodate the consumer, but may evaluate the consumer's application in accordance with its otherwise applicable underwriting criteria. The creditor may not deny the consumer's application or otherwise treat the consumer less favorably because the consumer specifically requested a medical accommodation, if the creditor would have extended the credit or treated the consumer more favorably under the creditor's otherwise applicable underwriting criteria.

(2) If a consumer applies for a loan by telephone and explains that his income has been and will continue to be interrupted on account of a medical condition and that he expects to repay the loan liquidating assets, the creditor may, but is not required to, evaluate the application using the sale of assets as the primary source of repayment, consistent with safe and sound practices, provided that the creditor documents the consumer's request by recording the oral conversation or making a notation of the request in the consumer's file.

(3) If a consumer applies for a loan and the application form provides a space where the consumer may provide any other information or special circumstances, whether medical or non-medical, that the consumer would like the creditor to consider in evaluating the consumer's application, the creditor may use medical information provided by the consumer in that space on that application to accommodate the consumer's application for credit, consistent with safe and sound practices, or may disregard that information.

(4) If a consumer specifically requests that the creditor use medical information in determining the consumer's eligibility, or continued eligibility, for credit and provides the creditor with medical information for that purpose, and the creditor determines that it needs additional information regarding the consumer's circumstances, the creditor may request, obtain, and use additional medical information about the consumer as necessary to verify the information provided by the consumer or to determine whether to make an accommodation for the consumer. The consumer may decline to provide additional information, withdraw the request for an accommodation, and have the application considered under the creditor's otherwise applicable underwriting criteria.

(5) If a consumer completes and signs a credit application that is not for medical purpose credit and the application contains boilerplate language that routinely requests medical information from the consumer or that indicates that by applying for credit the consumer authorizes or consents to the creditor obtaining and using medical information in connection with a determination of the consumer's eligibility, or continued eligibility, for credit, the consumer has not specifically requested that the creditor obtain and use medical information to accommodate the consumer's particular circumstances.

(e) *Example of a forbearance practice or program.* After an appropriate safety and soundness review, a creditor institutes a program that allows consumers who are or will be hospitalized to defer payments as needed for up to three months, without penalty, if the credit account has been open for more than one year and has not previously been in default, and the consumer provides confirming documentation at an appropriate time. A consumer is hospitalized and does not pay her bill for a particular month. This consumer has had a credit account with the creditor for more than one year and has not previously been in default. The creditor attempts to contact the consumer and speaks with the consumer's adult child, who is not the consumer's legal representative. The adult child informs the creditor that the consumer is hospitalized and is unable to pay the bill at that time. The creditor defers payments for up to three months, without penalty, for the hospitalized consumer and sends the consumer a letter confirming this practice and the date on which the next payment will be due.

Federal Deposit Insurance Corporation

12 CFR Chapter III.

Authority and Issuance

■ For the reasons set forth in the joint preamble, the Federal Deposit Insurance Corporation amends part 334 of chapter III of title 12 of the Code of Federal Regulations as follows:

PART 334—FAIR CREDIT REPORTING

■ 1. The authority citation for part 334 is revised to read as follows:

Authority: 12 U.S.C. 1819 (Tenth) and 1818; 15 U.S.C. 1681b and 1681s.

■ 2. Subpart A is added to part 334 to read as follows:

Subpart A—General Provisions

Sec.
334.1 [Reserved]
334.2 Examples.
334.3 Definitions.

Subpart A—General Provisions

§ 334.1 [Reserved]

§ 334.2 Examples.

The examples in this part are not exclusive. Compliance with an example, to the extent applicable, constitutes compliance with this part. Examples in a paragraph illustrate only the issue described in the paragraph and do not illustrate any other issue that may arise in this part.

§ 334.3 Definitions.

As used in this part, unless the context requires otherwise:

(a) *Act* means the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*).

(b) *Affiliate* means any company that is related by common ownership or common corporate control with another company.

(c) [Reserved]

(d) *Company* means any corporation, limited liability company, business

trust, general or limited partnership, association, or similar organization.

(e) *Consumer* means an individual.

(f) [Reserved]

(g) [Reserved]

(h) [Reserved]

(i) *Common ownership or common corporate control* means a relationship between two companies under which:

(1) One company has, with respect to the other company:

(i) Ownership, control, or power to vote 25 percent or more of the outstanding shares of any class of voting security of a company, directly or indirectly, or acting through one or more other persons;

(ii) Control in any manner over the election of a majority of the directors, trustees, or general partners (or individuals exercising similar functions) of a company; or

(iii) The power to exercise, directly or indirectly, a controlling influence over the management or policies of a company, as the FDIC determines; or

(2) Any other person has, with respect to both companies, a relationship described in paragraphs (i)(1)(i)–(i)(1)(iii) of this section.

(j) [Reserved]

(k) *Medical information* means:

(1) Information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to—

(i) The past, present, or future physical, mental, or behavioral health or condition of an individual;

(ii) The provision of health care to an individual; or

(iii) The payment for the provision of health care to an individual.

(2) The term does not include:

(i) The age or gender of a consumer;

(ii) Demographic information about the consumer, including a consumer's residence address or e-mail address;

(iii) Any other information about a consumer that does not relate to the physical, mental, or behavioral health or condition of a consumer, including the existence or value of any insurance policy; or

(iv) Information that does not identify a specific consumer.

(l) *Person* means any individual, partnership, corporation, trust, estate cooperative, association, government or governmental subdivision or agency, or other entity.

■ 3. Subpart D is added to part 334 to read as follows:

Subpart D—Medical Information

§ 334.30 Obtaining or using medical information in connection with a determination of eligibility for credit.

(a) *Scope.* This section applies to:

(1) Any of the following that participates as a creditor in a transaction—

(i) A State bank insured by the FDIC (other than members of the Federal Reserve System);

(ii) An insured State branch of a foreign bank; or

(2) Any other person that participates as a creditor in a transaction involving a person described in paragraph (a)(1) of this section.

(b) *General prohibition on obtaining or using medical information.* (1) *In general.* A creditor may not obtain or use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit, except as provided in this section.

(2) *Definitions.* (i) *Credit* has the same meaning as in section 702 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a.

(ii) *Creditor* has the same meaning as in section 702 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a.

(iii) *Eligibility, or continued eligibility, for credit* means the consumer's qualification or fitness to receive, or continue to receive, credit, including the terms on which credit is offered. The term does not include:

(A) Any determination of the consumer's qualification or fitness for employment, insurance (other than a credit insurance product), or other non-credit products or services;

(B) Authorizing, processing, or documenting a payment or transaction on behalf of the consumer in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit; or

(C) Maintaining or servicing the consumer's account in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit.

(c) *Rule of construction for obtaining and using unsolicited medical information.* (1) *In general.* A creditor does not obtain medical information in violation of the prohibition if it receives medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit without specifically requesting medical information.

(2) *Use of unsolicited medical information.* A creditor that receives unsolicited medical information in the manner described in paragraph (c)(1) of this section may use that information in connection with any determination of the consumer's eligibility, or continued eligibility, for credit to the extent the creditor can rely on at least one of the exceptions in § 334.30(d) or (e).

(3) *Examples.* A creditor does not obtain medical information in violation of the prohibition if, for example:

(i) In response to a general question regarding a consumer's debts or expenses, the creditor receives information that the consumer owes a debt to a hospital.

(ii) In a conversation with the creditor's loan officer, the consumer informs the creditor that the consumer has a particular medical condition.

(iii) In connection with a consumer's application for an extension of credit, the creditor requests a consumer report from a consumer reporting agency and receives medical information in the consumer report furnished by the agency even though the creditor did not specifically request medical information from the consumer reporting agency.

(d) *Financial information exception for obtaining and using medical information.* (1) *In general.* A creditor may obtain and use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit so long as:

(i) The information is the type of information routinely used in making credit eligibility determinations, such as information relating to debts, expenses, income, benefits, assets, collateral, or the purpose of the loan, including the use of proceeds;

(ii) The creditor uses the medical information in a manner and to an extent that is no less favorable than it would use comparable information that is not medical information in a credit transaction; and

(iii) The creditor does not take the consumer's physical, mental, or behavioral health, condition or history, type of treatment, or prognosis into account as part of any such determination.

(2) *Examples.* (i) *Examples of the types of information routinely used in making credit eligibility determinations.* Paragraph (d)(1)(i) of this section permits a creditor, for example, to obtain and use information about:

(A) The dollar amount, repayment terms, repayment history, and similar information regarding medical debts to calculate, measure, or verify the repayment ability of the consumer, the use of proceeds, or the terms for granting credit;

(B) The value, condition, and lien status of a medical device that may serve as collateral to secure a loan;

(C) The dollar amount and continued eligibility for disability income or benefits related to health or a medical condition that is relied on as a source of repayment; or

(D) The identity of creditors to whom outstanding medical debts are owed in connection with an application for credit, including but not limited to, a transaction involving the consolidation of medical debts.

(ii) *Examples of uses of medical information consistent with the exception.* (A) A consumer includes on an application for credit information about two $20,000 debts. One debt is to a hospital; the other debt is to a retailer. The creditor contacts the hospital and the retailer to verify the amount and payment status of the debts. The creditor learns that both debts are more than 90 days past due. Any two debts of this size that are more than 90 days past due would disqualify the consumer under the creditor's established underwriting criteria. The creditor denies the application on the basis that the consumer has a poor repayment history on outstanding debts. The creditor has used medical information in a manner and to an extent no less favorable than it would use comparable non-medical information.

(B) A consumer indicates on an application for a $200,000 mortgage loan that she receives $15,000 in long-term disability income each year from her former employer and has no other income. Annual income of $15,000, regardless of source, would not be sufficient to support the requested amount of credit. The creditor denies the application on the basis that the projected debt-to-income ratio of the consumer does not meet the creditor's underwriting criteria. The creditor has used medical information in a manner and to an extent that is no less favorable than it would use comparable non-medical information.

(C) A consumer includes on an application for a $10,000 home equity loan that he has a $50,000 debt to a medical facility that specializes in treating a potentially terminal disease. The creditor contacts the medical facility to verify the debt and obtain the repayment history and current status of the loan. The creditor learns that the debt is current. The applicant meets the income and other requirements of the creditor's underwriting guidelines. The creditor grants the application. The creditor has used medical information in accordance with the exception.

(iii) *Examples of uses of medical information inconsistent with the exception.* (A) A consumer applies for $25,000 of credit and includes on the application information about a $50,000 debt to a hospital. The creditor contacts the hospital to verify the amount and payment status of the debt, and learns that the debt is current and that the consumer has no delinquencies in her repayment history. If the existing debt were instead owed to a retail department store, the creditor would approve the application and extend credit based on the amount and repayment history of the outstanding debt. The creditor, however, denies the application because the consumer is indebted to a hospital. The creditor has used medical information, here the identity of the medical creditor, in a manner and to an extent that is less favorable than it would use comparable non-medical information.

(B) A consumer meets with a loan officer of a creditor to apply for a mortgage loan. While filling out the loan application, the consumer informs the loan officer orally that she has a potentially terminal disease. The consumer meets the creditor's established requirements for the requested mortgage loan. The loan officer recommends to the credit committee that the consumer be denied credit because the consumer has that disease. The credit committee follows the loan officer's recommendation and denies the application because the consumer has a potentially terminal disease. The creditor has used medical information in a manner inconsistent with the exception by taking into account the consumer's physical, mental, or behavioral health, condition, or history, type of treatment, or prognosis as part of a determination of eligibility or continued eligibility for credit.

(C) A consumer who has an apparent medical condition, such as a consumer who uses a wheelchair or an oxygen tank, meets with a loan officer to apply for a home equity loan. The consumer meets the creditor's established requirements for the requested home equity loan and the creditor typically does not require consumers to obtain a debt cancellation contract, debt suspension agreement, or credit insurance product in connection with such loans. However, based on the consumer's apparent medical condition, the loan officer recommends to the credit committee that credit be extended to the consumer only if the consumer obtains a debt cancellation contract, debt suspension agreement, or credit insurance product. The credit committee agrees with the loan officer's recommendation. The loan officer informs the consumer that the consumer must obtain a debt cancellation contract, debt suspension agreement, or credit insurance product to qualify for the loan. The consumer obtains one of these products from a third party and the creditor approves the loan. The creditor has used medical information in a manner inconsistent with the exception by taking into account the consumer's physical, mental, or behavioral health, condition, or history, type of treatment, or prognosis in setting conditions on the consumer's eligibility for credit.

(e) *Specific exceptions for obtaining and using medical information.* (1) *In general.* A creditor may obtain and use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit—

(i) To determine whether the use of a power of attorney or legal representative that is triggered by a medical event or condition is necessary and appropriate or whether the consumer has the legal capacity to contract when a person seeks to exercise a power of attorney or act as legal representative for a consumer based on an asserted medical event or condition;

(ii) To comply with applicable requirements of local, State, or Federal laws;

(iii) To determine, at the consumer's request, whether the consumer qualifies for a legally permissible special credit program or credit-related assistance program that is—

(A) Designed to meet the special needs of consumers with medical conditions; and

(B) Established and administered pursuant to a written plan that—

(*1*) Identifies the class of persons that the program is designed to benefit; and

(*2*) Sets forth the procedures and standards for extending credit or providing other credit-related assistance under the program.

(iv) To the extent necessary for purposes of fraud prevention or detection;

(v) In the case of credit for the purpose of financing medical products or services, to determine and verify the medical purpose of a loan and the use of proceeds;

(vi) Consistent with safe and sound practices, if the consumer or the consumer's legal representative specifically requests that the creditor use medical information in determining the consumer's eligibility, or continued eligibility, for credit, to accommodate the consumer's particular

circumstances, and such request is documented by the creditor;

(vii) Consistent with safe and sound practices, to determine whether the provisions of a forbearance practice or program that is triggered by a medical event or condition apply to a consumer;

(viii) To determine the consumer's eligibility for, the triggering of, or the reactivation of a debt cancellation contract or debt suspension agreement if a medical condition or event is a triggering event for the provision of benefits under the contract or agreement; or

(ix) To determine the consumer's eligibility for, the triggering of, or the reactivation of a credit insurance product if a medical condition or event is a triggering event for the provision of benefits under the product.

(2) *Example of determining eligibility for a special credit program or credit assistance program.* A not-for-profit organization establishes a credit assistance program pursuant to a written plan that is designed to assist disabled veterans in purchasing homes by subsidizing the down payment for the home purchase mortgage loans of qualifying veterans. The organization works through mortgage lenders and requires mortgage lenders to obtain medical information about the disability of any consumer that seeks to qualify for the program, use that information to verify the consumer's eligibility for the program, and forward that information to the organization. A consumer who is a veteran applies to a creditor for a home purchase mortgage loan. The creditor informs the consumer about the credit assistance program for disabled veterans and the consumer seeks to qualify for the program. Assuming that the program complies with all applicable law, including applicable fair lending laws, the creditor may obtain and use medical information about the medical condition and disability, if any, of the consumer to determine whether the consumer qualifies for the credit assistance program.

(3) *Examples of verifying the medical purpose of the loan or the use of proceeds.* (i) If a consumer applies for $10,000 of credit for the purpose of financing vision correction surgery, the creditor may verify with the surgeon that the procedure will be performed. If the surgeon reports that surgery will not be performed on the consumer, the creditor may use that medical information to deny the consumer's application for credit, because the loan would not be used for the stated purpose.

(ii) If a consumer applies for $10,000 of credit for the purpose of financing cosmetic surgery, the creditor may confirm the cost of the procedure with the surgeon. If the surgeon reports that the cost of the procedure is $5,000, the creditor may use that medical information to offer the consumer only $5,000 of credit.

(iii) A creditor has an established medical loan program for financing particular elective surgical procedures. The creditor receives a loan application from a consumer requesting $10,000 of credit under the established loan program for an elective surgical procedure. The consumer indicates on the application that the purpose of the loan is to finance an elective surgical procedure not eligible for funding under the guidelines of the established loan program. The creditor may deny the consumer's application because the purpose of the loan is not for a particular procedure funded by the established loan program.

(4) *Examples of obtaining and using medical information at the request of the consumer.* (i) If a consumer applies for a loan and specifically requests that the creditor consider the consumer's medical disability at the relevant time as an explanation for adverse payment history information in his credit report, the creditor may consider such medical information in evaluating the consumer's willingness and ability to repay the requested loan to accommodate the consumer's particular circumstances, consistent with safe and sound practices. The creditor may also decline to consider such medical information to accommodate the consumer, but may evaluate the consumer's application in accordance with its otherwise applicable underwriting criteria. The creditor may not deny the consumer's application or otherwise treat the consumer less favorably because the consumer specifically requested a medical accommodation, if the creditor would have extended the credit or treated the consumer more favorably under the creditor's otherwise applicable underwriting criteria.

(ii) If a consumer applies for a loan by telephone and explains that his income has been and will continue to be interrupted on account of a medical condition and that he expects to repay the loan by liquidating assets, the creditor may, but is not required to, evaluate the application using the sale of assets as the primary source of repayment, consistent with safe and sound practices, provided that the creditor documents the consumer's request by recording the oral conversation or making a notation of the request in the consumer's file.

(iii) If a consumer applies for a loan and the application form provides a space where the consumer may provide any other information or special circumstances, whether medical or non-medical, that the consumer would like the creditor to consider in evaluating the consumer's application, the creditor may use medical information provided by the consumer in that space on that application to accommodate the consumer's application for credit, consistent with safe and sound practices, or may disregard that information.

(iv) If a consumer specifically requests that the creditor use medical information in determining the consumer's eligibility, or continued eligibility, for credit and provides the creditor with medical information for that purpose, and the creditor determines that it needs additional information regarding the consumer's circumstances, the creditor may request, obtain, and use additional medical information about the consumer as necessary to verify the information provided by the consumer or to determine whether to make an accommodation for the consumer. The consumer may decline to provide additional information, withdraw the request for an accommodation, and have the application considered under the creditor's otherwise applicable underwriting criteria.

(v) If a consumer completes and signs a credit application that is not for medical purpose credit and the application contains boilerplate language that routinely requests medical information from the consumer or that indicates that by applying for credit the consumer authorizes or consents to the creditor obtaining and using medical information in connection with a determination of the consumer's eligibility, or continued eligibility, for credit, the consumer has not specifically requested that the creditor obtain and use medical information to accommodate the consumer's particular circumstances.

(5) *Example of a forbearance practice or program.* After an appropriate safety and soundness review, a creditor institutes a program that allows consumers who are or will be hospitalized to defer payments as needed for up to three months, without penalty, if the credit account has been open for more than one year and has not previously been in default, and the consumer provides confirming documentation at an appropriate time. A consumer is hospitalized and does not pay her bill for a particular month. This consumer has had a credit account

with the creditor for more than one year and has not previously been in default. The creditor attempts to contact the consumer and speaks with the consumer's adult child, who is not the consumer's legal representative. The adult child informs the creditor that the consumer is hospitalized and is unable to pay the bill at that time. The creditor defers payments for up to three months, without penalty, for the hospitalized consumer and sends the consumer a letter confirming this practice and the date on which the next payment will be due.

§ 334.31 Limits on redisclosure of information.

(a) *Scope.* This section applies to State banks insured by the FDIC (other than members of the Federal Reserve System) and insured State branches of foreign banks.

(b) *Limits on redisclosure.* If a person described in paragraph (a) of this section receives medical information about a consumer from a consumer reporting agency or its affiliate, the person must not disclose that information to any other person, except as necessary to carry out the purpose for which the information was initially disclosed, or as otherwise permitted by statute, regulation, or order.

§ 334.32 Sharing medical information with affiliates.

(a) *Scope.* This section applies to State banks insured by the FDIC (other than members of the Federal Reserve System) and insured State branches of foreign banks.

(b) *In general.* The exclusions from the term ''consumer report'' in section 603(d)(2) of the Act that allow the sharing of information with affiliates do not apply if a person described in paragraph (a) of this section communicates to an affiliate—

(1) Medical information;

(2) An individualized list or description based on the payment transactions of the consumer for medical products or services; or

(3) An aggregate list of identified consumers based on payment transactions for medical products or services.

(c) *Exceptions.* A person described in paragraph (a) of this section may rely on the exclusions from the term ''consumer report'' in section 603(d)(2) of the Act to communicate the information in paragraph (b) of this section to an affiliate—

(1) In connection with the business of insurance or annuities (including the activities described in section 18B of the model Privacy of Consumer Financial and Health Information Regulation issued by the National Association of Insurance Commissioners, as in effect on January 1, 2003);

(2) For any purpose permitted without authorization under the regulations promulgated by the Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA);

(3) For any purpose referred to in section 1179 of HIPAA;

(4) For any purpose described in section 502(e) of the Gramm-Leach-Bliley Act;

(5) In connection with a determination of the consumer's eligibility, or continued eligibility, for credit consistent with § 334.30; or

(6) As otherwise permitted by order of the FDIC.

Office of Thrift Supervision

12 CFR Chapter V.

Authority and Issuance

■ For the reasons set forth in the joint preamble, the Office of Thrift Supervision amends chapter V of title 12 of the Code of Federal Regulations as follows:

PART 571—FAIR CREDIT REPORTING

■ 1. The authority citation for part 571 is revised to read as follows:

Authority: 12 U.S.C. 1462a, 1463, 1464, 1467a, 1828, 1831p–1, and 1881–1884; 15 U.S.C. 1681b, 1681s, and 1681w; 15 U.S.C. 6801 and 6805(b)(1).

Subpart A—General Provisions

■ 2. Revise § 571.1(b)(2) to read as follows:

§ 571.1 Purpose and Scope.

* * * * *

(b) * * *

(2) *Scope in general.* Except as otherwise provided in this part, this part applies to savings associations whose deposits are insured by the Federal Deposit Insurance Corporation (and Federal savings association operating subsidiaries in accordance with § 559.3(h)(1) of this chapter).

■ 3. Add § 571.2 to read as follows:

§ 571.2 Examples.

The examples in this part are not exclusive. Compliance with an example, to the extent applicable, constitutes compliance with this part. Examples in a paragraph illustrate only the issue described in the paragraph and do not illustrate any other issue that may arise in this part.

■ 4. Amend § 571.3 by revising the introductory text and paragraphs (a) through (n) to read as follows:

§ 571.3 Definitions.

As used in this part, unless the context requires otherwise:

(a) *Act* means the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*).

(b) *Affiliate* means any company that is related by common ownership or common corporate control with another company.

(c) [Reserved]

(d) *Company* means any corporation, limited liability company, business trust, general or limited partnership, association, or similar organization.

(e) *Consumer* means an individual.

(f)–(h) [Reserved]

(i) *Common ownership or common corporate control* means a relationship between two companies under which:

(1) One company has, with respect to the other company:

(i) Ownership, control, or power to vote 25 percent or more of the outstanding shares of any class of voting security of a company, directly or indirectly, or acting through one or more other persons;

(ii) Control in any manner over the election of a majority of the directors, trustees, or general partners (or individuals exercising similar functions) of a company; or

(iii) The power to exercise, directly or indirectly, a controlling influence over the management or policies of a company, as the OTS determines; or

(2) Any other person has, with respect to both companies, a relationship described in paragraphs (i)(1)(i)–(i)(1)(iii) of this section.

(j) [Reserved]

(k) *Medical information* means:

(1) Information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to—

(i) The past, present, or future physical, mental, or behavioral health or condition of an individual;

(ii) The provision of health care to an individual; or

(iii) The payment for the provision of health care to an individual.

(2) The term does not include:

(i) The age or gender of a consumer;

(ii) Demographic information about the consumer, including a consumer's residence address or e-mail address;

(iii) Any other information about a consumer that does not relate to the physical, mental, or behavioral health or condition of a consumer, including the existence or value of any insurance policy; or

(iv) Information that does not identify a specific consumer.

(l) *Person* means any individual, partnership, corporation, trust, estate

cooperative, association, government or governmental subdivision or agency, or other entity.

(m)–(n) [Reserved]

* * * * *

■ 5. Add subpart D to part 571 to read as follows:

Subpart D—Medical Information

§ 571.30 Obtaining or using medical information in connection with a determination of eligibility for credit.

(a) *Scope.* This section applies to:

(1) Any of the following that participates as a creditor in a transaction—

(i) A savings association;

(ii) A subsidiary owned in whole or in part by a savings association;

(iii) A savings and loan holding company;

(iv) A subsidiary of a savings and loan holding company other than a bank or subsidiary of a bank; or

(v) A service corporation owned in whole or in part by a savings association; or

(2) Any other person that participates as a creditor in a transaction involving a person described in paragraph (a)(1) of this section.

(b) *General prohibition on obtaining or using medical information.* (1) *In general.* A creditor may not obtain or use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit, except as provided in this section.

(2) *Definitions.* (i) *Credit* has the same meaning as in section 702 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a.

(ii) *Creditor* has the same meaning as in section 702 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a.

(iii) *Eligibility, or continued eligibility, for credit* means the consumer's qualification or fitness to receive, or continue to receive, credit, including the terms on which credit is offered. The term does not include:

(A) Any determination of the consumer's qualification or fitness for employment, insurance (other than a credit insurance product), or other non-credit products or services;

(B) Authorizing, processing, or documenting a payment or transaction on behalf of the consumer in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit; or

(C) Maintaining or servicing the consumer's account in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit.

(c) *Rule of construction for obtaining and using unsolicited medical information.* (1) *In general.* A creditor does not obtain medical information in violation of the prohibition if it receives medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit without specifically requesting medical information.

(2) *Use of unsolicited medical information.* A creditor that receives unsolicited medical information in the manner described in paragraph (c)(1) of this section may use that information in connection with any determination of the consumer's eligibility, or continued eligibility, for credit to the extent the creditor can rely on at least one of the exceptions in § 571.30(d) or (e).

(3) *Examples.* A creditor does not obtain medical information in violation of the prohibition if, for example:

(i) In response to a general question regarding a consumer's debts or expenses, the creditor receives information that the consumer owes a debt to a hospital;

(ii) In a conversation with the creditor's loan officer, the consumer informs the creditor that the consumer has a particular medical condition; or

(iii) In connection with a consumer's application for an extension of credit, the creditor requests a consumer report from a consumer reporting agency and receives medical information in the consumer report furnished by the agency even though the creditor did not specifically request medical information from the consumer reporting agency.

(d) *Financial information exception for obtaining and using medical information.* (1) *In general.* A creditor may obtain and use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit so long as:

(i) The information is the type of information routinely used in making credit eligibility determinations, such as information relating to debts, expenses, income, benefits, assets, collateral, or the purpose of the loan, including the use of proceeds;

(ii) The creditor uses the medical information in a manner and to an extent that is no less favorable than it would use comparable information that is not medical information in a credit transaction; and

(iii) The creditor does not take the consumer's physical, mental, or behavioral health, condition or history, type of treatment, or prognosis into account as part of any such determination.

(2) *Examples.* (i) *Examples of the types of information routinely used in making credit eligibility determinations.* Paragraph (d)(1)(i) of this section permits a creditor, for example, to obtain and use information about:

(A) The dollar amount, repayment terms, repayment history, and similar information regarding medical debts to calculate, measure, or verify the repayment ability of the consumer, the use of proceeds, or the terms for granting credit;

(B) The value, condition, and lien status of a medical device that may serve as collateral to secure a loan;

(C) The dollar amount and continued eligibility for disability income or benefits related to health or a medical condition that is relied on as a source of repayment; or

(D) The identity of creditors to whom outstanding medical debts are owed in connection with an application for credit, including but not limited to, a transaction involving the consolidation of medical debts.

(ii) *Examples of uses of medical information consistent with the exception.* (A) A consumer includes on an application for credit information about two $20,000 debts. One debt is to a hospital; the other debt is to a retailer. The creditor contacts the hospital and the retailer to verify the amount and payment status of the debts. The creditor learns that both debts are more than 90 days past due. Any two debts of this size that are more than 90 days past due would disqualify the consumer under the creditor's established underwriting criteria. The creditor denies the application on the basis that the consumer has a poor repayment history on outstanding debts. The creditor has used medical information in a manner and to an extent no less favorable than it would use comparable non-medical information.

(B) A consumer indicates on an application for a $200,000 mortgage loan that she receives $15,000 in long-term disability income each year from her former employer and has no other income. Annual income of $15,000, regardless of source, would not be sufficient to support the requested amount of credit. The creditor denies the application on the basis that the projected debt-to-income ratio of the consumer does not meet the creditor's underwriting criteria. The creditor has used medical information in a manner and to an extent that is no less favorable than it would use comparable non-medical information.

(C) A consumer includes on an application for a $10,000 home equity loan that he has a $50,000 debt to a

medical facility that specializes in treating a potentially terminal disease. The creditor contacts the medical facility to verify the debt and obtain the repayment history and current status of the loan. The creditor learns that the debt is current. The applicant meets the income and other requirements of the creditor's underwriting guidelines. The creditor grants the application. The creditor has used medical information in accordance with the exception.

(iii) *Examples of uses of medical information inconsistent with the exception.* (A) A consumer applies for $25,000 of credit and includes on the application information about a $50,000 debt to a hospital. The creditor contacts the hospital to verify the amount and payment status of the debt, and learns that the debt is current and that the consumer has no delinquencies in her repayment history. If the existing debt were instead owed to a retail department store, the creditor would approve the application and extend credit based on the amount and repayment history of the outstanding debt. The creditor, however, denies the application because the consumer is indebted to a hospital. The creditor has used medical information, here the identity of the medical creditor, in a manner and to an extent that is less favorable than it would use comparable non-medical information.

(B) A consumer meets with a loan officer of a creditor to apply for a mortgage loan. While filling out the loan application, the consumer informs the loan officer orally that she has a potentially terminal disease. The consumer meets the creditor's established requirements for the requested mortgage loan. The loan officer recommends to the credit committee that the consumer be denied credit because the consumer has that disease. The credit committee follows the loan officer's recommendation and denies the application because the consumer has a potentially terminal disease. The creditor has used medical information in a manner inconsistent with the exception by taking into account the consumer's physical, mental, or behavioral health, condition, or history, type of treatment, or prognosis as part of a determination of eligibility or continued eligibility for credit.

(C) A consumer who has an apparent medical condition, such as a consumer who uses a wheelchair or an oxygen tank, meets with a loan officer to apply for a home equity loan. The consumer meets the creditor's established requirements for the requested home equity loan and the creditor typically does not require consumers to obtain a debt cancellation contract, debt suspension agreement, or credit insurance product in connection with such loans. However, based on the consumer's apparent medical condition, the loan officer recommends to the credit committee that credit be extended to the consumer only if the consumer obtains a debt cancellation contract, debt suspension agreement, or credit insurance product. The credit committee agrees with the loan officer's recommendation. The loan officer informs the consumer that the consumer must obtain a debt cancellation contract, debt suspension agreement, or credit insurance product to qualify for the loan. The consumer obtains one of these products from a third party and the creditor approves the loan. The creditor has used medical information in a manner inconsistent with the exception by taking into account the consumer's physical, mental, or behavioral health, condition, or history, type of treatment, or prognosis in setting conditions on the consumer's eligibility for credit.

(e) *Specific exceptions for obtaining and using medical information.* (1) *In general.* A creditor may obtain and use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit—

(i) To determine whether the use of a power of attorney or legal representative that is triggered by a medical event or condition is necessary and appropriate or whether the consumer has the legal capacity to contract when a person seeks to exercise a power of attorney or act as legal representative for a consumer based on an asserted medical event or condition;

(ii) To comply with applicable requirements of local, State, or Federal laws;

(iii) To determine, at the consumer's request, whether the consumer qualifies for a legally permissible special credit program or credit-related assistance program that is—

(A) Designed to meet the special needs of consumers with medical conditions; and

(B) Established and administered pursuant to a written plan that—

(*1*) Identifies the class of persons that the program is designed to benefit; and

(*2*) Sets forth the procedures and standards for extending credit or providing other credit-related assistance under the program.

(iv) To the extent necessary for purposes of fraud prevention or detection;

(v) In the case of credit for the purpose of financing medical products or services, to determine and verify the medical purpose of a loan and the use of proceeds;

(vi) Consistent with safe and sound practices, if the consumer or the consumer's legal representative specifically requests that the creditor use medical information in determining the consumer's eligibility, or continued eligibility, for credit, to accommodate the consumer's particular circumstances, and such request is documented by the creditor;

(vii) Consistent with safe and sound practices, to determine whether the provisions of a forbearance practice or program that is triggered by a medical event or condition apply to a consumer;

(viii) To determine the consumer's eligibility for, the triggering of, or the reactivation of a debt cancellation contract or debt suspension agreement if a medical condition or event is a triggering event for the provision of benefits under the contract or agreement; or

(ix) To determine the consumer's eligibility for, the triggering of, or the reactivation of a credit insurance product if a medical condition or event is a triggering event for the provision of benefits under the product.

(2) *Example of determining eligibility for a special credit program or credit assistance program.* A not-for-profit organization establishes a credit assistance program pursuant to a written plan that is designed to assist disabled veterans in purchasing homes by subsidizing the down payment for the home purchase mortgage loans of qualifying veterans. The organization works through mortgage lenders and requires mortgage lenders to obtain medical information about the disability of any consumer that seeks to qualify for the program, use that information to verify the consumer's eligibility for the program, and forward that information to the organization. A consumer who is a veteran applies to a creditor for a home purchase mortgage loan. The creditor informs the consumer about the credit assistance program for disabled veterans and the consumer seeks to qualify for the program. Assuming that the program complies with all applicable law, including applicable fair lending laws, the creditor may obtain and use medical information about the medical condition and disability, if any, of the consumer to determine whether the consumer qualifies for the credit assistance program.

(3) *Examples of verifying the medical purpose of the loan or the use of proceeds.* (i) If a consumer applies for

$10,000 of credit for the purpose of financing vision correction surgery, the creditor may verify with the surgeon that the procedure will be performed. If the surgeon reports that surgery will not be performed on the consumer, the creditor may use that medical information to deny the consumer's application for credit, because the loan would not be used for the stated purpose.

(ii) If a consumer applies for $10,000 of credit for the purpose of financing cosmetic surgery, the creditor may confirm the cost of the procedure with the surgeon. If the surgeon reports that the cost of the procedure is $5,000, the creditor may use that medical information to offer the consumer only $5,000 of credit.

(iii) A creditor has an established medical loan program for financing particular elective surgical procedures. The creditor receives a loan application from a consumer requesting $10,000 of credit under the established loan program for an elective surgical procedure. The consumer indicates on the application that the purpose of the loan is to finance an elective surgical procedure not eligible for funding under the guidelines of the established loan program. The creditor may deny the consumer's application because the purpose of the loan is not for a particular procedure funded by the established loan program.

(4) *Examples of obtaining and using medical information at the request of the consumer.* (i) If a consumer applies for a loan and specifically requests that the creditor consider the consumer's medical disability at the relevant time as an explanation for adverse payment history information in his credit report, the creditor may consider such medical information in evaluating the consumer's willingness and ability to repay the requested loan to accommodate the consumer's particular circumstances, consistent with safe and sound practices. The creditor may also decline to consider such medical information to accommodate the consumer, but may evaluate the consumer's application in accordance with its otherwise applicable underwriting criteria. The creditor may not deny the consumer's application or otherwise treat the consumer less favorably because the consumer specifically requested a medical accommodation, if the creditor would have extended the credit or treated the consumer more favorably under the creditor's otherwise applicable underwriting criteria.

(ii) If a consumer applies for a loan by telephone and explains that his income has been and will continue to be interrupted on account of a medical condition and that he expects to repay the loan by liquidating assets, the creditor may, but is not required to, evaluate the application using the sale of assets as the primary source of repayment, consistent with safe and sound practices, provided that the creditor documents the consumer's request by recording the oral conversation or making a notation of the request in the consumer's file.

(iii) If a consumer applies for a loan and the application form provides a space where the consumer may provide any other information or special circumstances, whether medical or non-medical, that the consumer would like the creditor to consider in evaluating the consumer's application, the creditor may use medical information provided by the consumer in that space on that application to accommodate the consumer's application for credit, consistent with safe and sound practices, or may disregard that information.

(iv) If a consumer specifically requests that the creditor use medical information in determining the consumer's eligibility, or continued eligibility, for credit and provides the creditor with medical information for that purpose, and the creditor determines that it needs additional information regarding the consumer's circumstances, the creditor may request, obtain, and use additional medical information about the consumer as necessary to verify the information provided by the consumer or to determine whether to make an accommodation for the consumer. The consumer may decline to provide additional information, withdraw the request for an accommodation, and have the application considered under the creditor's otherwise applicable underwriting criteria.

(v) If a consumer completes and signs a credit application that is not for medical purpose credit and the application contains boilerplate language that routinely requests medical information from the consumer or that indicates that by applying for credit the consumer authorizes or consents to the creditor obtaining and using medical information in connection with a determination of the consumer's eligibility, or continued eligibility, for credit, the consumer has not specifically requested that the creditor obtain and use medical information to accommodate the consumer's particular circumstances.

(5) *Example of a forbearance practice or program.* After an appropriate safety and soundness review, a creditor institutes a program that allows consumers who are or will be hospitalized to defer payments as needed for up to three months, without penalty, if the credit account has been open for more than one year and has not previously been in default, and the consumer provides confirming documentation at an appropriate time. A consumer is hospitalized and does not pay her bill for a particular month. This consumer has had a credit account with the creditor for more than one year and has not previously been in default. The creditor attempts to contact the consumer and speaks with the consumer's spouse, who is not the consumer's legal representative. The spouse informs the creditor that the consumer is hospitalized and is unable to pay the bill at that time. The creditor defers payments for up to three months, without penalty, for the hospitalized consumer and sends the consumer a letter confirming this practice and the date on which the next payment will be due.

§ 571.31 Limits on redisclosure of information.

(a) *Scope.* This section applies to savings associations and federal savings association operating subsidiaries.

(b) *Limits on redisclosure.* If a person described in paragraph (a) of this section receives medical information about a consumer from a consumer reporting agency or its affiliate, the person must not disclose that information to any other person, except as necessary to carry out the purpose for which the information was initially disclosed, or as otherwise permitted by statute, regulation, or order.

§ 571.32 Sharing medical information with affiliates.

(a) *Scope.* This section applies to savings associations and Federal savings association operating subsidiaries.

(b) *In general.* The exclusions from the term ''consumer report'' in section 603(d)(2) of the Act that allow the sharing of information with affiliates do not apply if a person described in paragraph (a) of this section communicates to an affiliate—

(1) Medical information;

(2) An individualized list or description based on the payment transactions of the consumer for medical products or services; or

(3) An aggregate list of identified consumers based on payment transactions for medical products or services.

(c) *Exceptions.* A person described in paragraph (a) of this section may rely on

the exclusions from the term ''consumer report'' in section 603(d)(2) of the Act to communicate the information in paragraph (b) of this section to an affiliate—

(1) In connection with the business of insurance or annuities (including the activities described in section 18B of the model Privacy of Consumer Financial and Health Information Regulation issued by the National Association of Insurance Commissioners, as in effect on January 1, 2003);

(2) For any purpose permitted without authorization under the regulations promulgated by the Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA);

(3) For any purpose referred to in section 1179 of HIPAA;

(4) For any purpose described in section 502(e) of the Gramm-Leach-Bliley Act;

(5) In connection with a determination of the consumer's eligibility, or continued eligibility, for credit consistent with § 571.30; or

(6) As otherwise permitted by order of the OTS.

National Credit Union Administration

■ For the reasons set out in the preamble, 12 CFR chapter VII is amended as follows:

PART 717—FAIR CREDIT REPORTING

■ 1. Revise the authority citation for part 717 to read as follows:

Authority: 15 U.S.C. 1681a, 1681b, 1681s, 1681w, 6801 and 6805.

■ 2. Amend part 717 by revising subpart A to read as follows:

Subpart A—General Provisions

Subpart A—General Provisions

§ 717.1 Purpose.

(a) *Purpose.* The purpose of this part is to establish standards for Federal credit unions regarding consumer report information. In addition, the purpose of this part is to specify the extent to which Federal credit unions may obtain, use or share certain information. This part also contains a number of measures Federal credit unions must take to combat consumer fraud and related crimes, including identity theft.

(b) [Reserved]

§ 717.2 Examples.

The examples in this part are not exclusive. Compliance with an example, to the extent applicable, constitutes compliance with this part. Examples in a paragraph illustrate only the issue described in the paragraph and do not illustrate any other issue that may arise in this part.

§ 717.3 Definitions.

As used in this part, unless the context requires otherwise:

(a) *Act* means the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*).

(b) *Affiliate* means any company that is related by common ownership or common corporate control with another company. For example, an affiliate of a Federal credit union is a credit union service corporation (CUSO), as provided in 12 CFR part 712, that is controlled by the Federal credit union.

(c) [Reserved]

(d) *Company* means any corporation, limited liability company, business trust, general or limited partnership, association, or similar organization.

(e) *Consumer* means an individual.

(f) [Reserved]

(g) [Reserved]

(h) [Reserved]

(i) *Common ownership or common corporate control* means a relationship between two companies under which:

(1) One company has, with respect to the other company:

(i) Ownership, control, or power to vote 25 percent or more of the outstanding shares of any class of voting security of a company, directly or indirectly, or acting through one or more other persons;

(ii) Control in any manner over the election of a majority of the directors, trustees, or general partners (or individuals exercising similar functions) of a company; or

(iii) The power to exercise, directly or indirectly, a controlling influence over the management or policies of a company, as the NCUA determines; or

(iv) Example. NCUA will presume a credit union has a controlling influence over the management or policies of a CUSO, if the CUSO is 67% owned by credit unions.

(2) Any other person has, with respect to both companies, a relationship described in paragraphs (i)(1)(i)–(i)(1)(iii) of this section.

(j) [Reserved]

(k) *Medical information* means:

(l) Information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to—

(i) The past, present, or future physical, mental, or behavioral health or condition of an individual;

(ii) The provision of health care to an individual; or

(iii) The payment for the provision of health care to an individual.

(2) The term does not include:

(i) The age or gender of a consumer;

(ii) Demographic information about the consumer, including a consumer's residence address or e-mail address;

(iii) Any other information about a consumer that does not relate to the physical, mental, or behavioral health or condition of a consumer, including the existence or value of any insurance policy; or

(iv) Information that does not identify a specific consumer.

(l) *Person* means any individual, partnership, corporation, trust, estate cooperative, association, government or governmental subdivision or agency, or other entity.

■ 3. Subpart D is added to part 717 to read as follows:

Subpart D—Medical Information

§ 717.30 Obtaining or using medical information in connection with a determination of eligibility for credit.

(a) *Scope.* This section applies to:

(1) A Federal credit union that participates as a creditor in a transaction; or

(2) Any other person that participates as a creditor in a transaction involving a person described in paragraph (1).

(b) *General prohibition on obtaining or using medical information.* (1) *In general.* A creditor may not obtain or use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit, except as provided in this section.

(2) *Definitions.* (i) *Credit* has the same meaning as in section 702 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a.

(ii) *Creditor* has the same meaning as in section 702 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a.

(iii) *Eligibility, or continued eligibility, for credit* means the consumer's qualification or fitness to receive, or continue to receive, credit, including the terms on which credit is offered. The term does not include:

(A) Any determination of the consumer's qualification or fitness for employment, insurance (other than a credit insurance product), or other non-credit products or services;

(B) Authorizing, processing, or documenting a payment or transaction on behalf of the consumer in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit; or

(C) Maintaining or servicing the consumer's account in a manner that

does not involve a determination of the consumer's eligibility, or continued eligibility, for credit.

(c) *Rule of construction for obtaining and using unsolicited medical information.* (1) *In general.* A creditor does not obtain medical information in violation of the prohibition if it receives medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit without specifically requesting medical information.

(2) *Use of unsolicited medical information.* A creditor that receives unsolicited medical information in the manner described in paragraph (1) may use that information in connection with any determination of the consumer's eligibility, or continued eligibility, for credit to the extent the creditor can rely on at least one of the exceptions in § 717.30(d) or (e).

(3) *Examples.* A creditor does not obtain medical information in violation of the prohibition if, for example:

(i) In response to a general question regarding a consumer's debts or expenses, the creditor receives information that the consumer owes a debt to a hospital.

(ii) In a conversation with the creditor's loan officer, the consumer informs the creditor that the consumer has a particular medical condition.

(iii) In connection with a consumer's application for an extension of credit, the creditor requests a consumer report from a consumer reporting agency and receives medical information in the consumer report furnished by the agency even though the creditor did not specifically request medical information from the consumer reporting agency.

(d) *Financial information exception for obtaining and using medical information.*

(1) *In general.* A creditor may obtain and use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit so long as:

(i) The information is the type of information routinely used in making credit eligibility determinations, such as information relating to debts, expenses, income, benefits, assets, collateral, or the purpose of the loan, including the use of proceeds;

(ii) The creditor uses the medical information in a manner and to an extent that is no less favorable than it would use comparable information that is not medical information in a credit transaction; and

(iii) The creditor does not take the consumer's physical, mental, or behavioral health, condition or history, type of treatment, or prognosis into account as part of any such determination.

(2) *Examples.* (i) *Examples of the types of information routinely used in making credit eligibility determinations.* Paragraph (d)(1)(i) of this section permits a creditor, for example, to obtain and use information about:

(A) The dollar amount, repayment terms, repayment history, and similar information regarding medical debts to calculate, measure, or verify the repayment ability of the consumer, the use of proceeds, or the terms for granting credit;

(B) The value, condition, and lien status of a medical device that may serve as collateral to secure a loan;

(C) The dollar amount and continued eligibility for disability income or benefits related to health or a medical condition that is relied on as a source of repayment; or

(D) The identity of creditors to whom outstanding medical debts are owed in connection with an application for credit, including but not limited to, a transaction involving the consolidation of medical debts.

(ii) *Examples of uses of medical information consistent with the exception.* (A) A consumer includes on an application for credit information about two $20,000 debts. One debt is to a hospital; the other debt is to a retailer. The creditor contacts the hospital and the retailer to verify the amount and payment status of the debts. The creditor learns that both debts are more than 90 days past due. Any two debts of this size that are more than 90 days past due would disqualify the consumer under the creditor's established underwriting criteria. The creditor denies the application on the basis that the consumer has a poor repayment history on outstanding debts. The creditor has used medical information in a manner and to an extent no less favorable than it would use comparable non-medical information.

(B) A consumer indicates on an application for a $200,000 mortgage loan that she receives $15,000 in long-term disability income each year from her former employer and has no other income. Annual income of $15,000, regardless of source, would not be sufficient to support the requested amount of credit. The creditor denies the application on the basis that the projected debt-to-income ratio of the consumer does not meet the creditor's underwriting criteria. The creditor has used medical information in a manner and to an extent that is no less favorable than it would use comparable non-medical information.

(C) A consumer includes on an application for a $10,000 home equity loan that he has a $50,000 debt to a medical facility that specializes in treating a potentially terminal disease. The creditor contacts the medical facility to verify the debt and obtain the repayment history and current status of the loan. The creditor learns that the debt is current. The applicant meets the income and other requirements of the creditor's underwriting guidelines. The creditor grants the application. The creditor has used medical information in accordance with the exception.

(iii) *Examples of uses of medical information inconsistent with the exception.* (A) A consumer applies for $25,000 of credit and includes on the application information about a $50,000 debt to a hospital. The creditor contacts the hospital to verify the amount and payment status of the debt, and learns that the debt is current and that the consumer has no delinquencies in her repayment history. If the existing debt were instead owed to a retail department store, the creditor would approve the application and extend credit based on the amount and repayment history of the outstanding debt. The creditor, however, denies the application because the consumer is indebted to a hospital. The creditor has used medical information, here the identity of the medical creditor, in a manner and to an extent that is less favorable than it would use comparable non-medical information.

(B) A consumer meets with a loan officer of a creditor to apply for a mortgage loan. While filling out the loan application, the consumer informs the loan officer orally that she has a potentially terminal disease. The consumer meets the creditor's established requirements for the requested mortgage loan. The loan officer recommends to the credit committee that the consumer be denied credit because the consumer has that disease. The credit committee follows the loan officer's recommendation and denies the application because the consumer has a potentially terminal disease. The creditor has used medical information in a manner inconsistent with the exception by taking into account the consumer's physical, mental, or behavioral health, condition, or history, type of treatment, or prognosis as part of a determination of eligibility or continued eligibility for credit.

(C) A consumer who has an apparent medical condition, such as a consumer who uses a wheelchair or an oxygen

tank, meets with a loan officer to apply for a home equity loan. The consumer meets the creditor's established requirements for the requested home equity loan and the creditor typically does not require consumers to obtain a debt cancellation contract, debt suspension agreement, or credit insurance product in connection with such loans. However, based on the consumer's apparent medical condition, the loan officer recommends to the credit committee that credit be extended to the consumer only if the consumer obtains a debt cancellation contract, debt suspension agreement, or credit insurance product. The credit committee agrees with the loan officer's recommendation. The loan officer informs the consumer that the consumer must obtain a debt cancellation contract, debt suspension agreement, or credit insurance product to qualify for the loan. The consumer obtains one of these products from a third party and the creditor approves the loan. The creditor has used medical information in a manner inconsistent with the exception by taking into account the consumer's physical, mental, or behavioral health, condition, or history, type of treatment, or prognosis in setting conditions on the consumer's eligibility for credit.

(e) *Specific exceptions for obtaining and using medical information.* (1) *In general.* A creditor may obtain and use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit—

(i) To determine whether the use of a power of attorney or legal representative that is triggered by a medical event or condition is necessary and appropriate or whether the consumer has the legal capacity to contract when a person seeks to exercise a power of attorney or act as legal representative for a consumer based on an asserted medical event or condition;

(ii) To comply with applicable requirements of local, State, or Federal laws;

(iii) To determine, at the consumer's request, whether the consumer qualifies for a legally permissible special credit program or credit-related assistance program that is—

(A) Designed to meet the special needs of consumers with medical conditions; and

(B) Established and administered pursuant to a written plan that—

(*1*) Identifies the class of persons that the program is designed to benefit; and

(*2*) Sets forth the procedures and standards for extending credit or providing other credit-related assistance under the program.

(iv) To the extent necessary for purposes of fraud prevention or detection;

(v) In the case of credit for the purpose of financing medical products or services, to determine and verify the medical purpose of a loan and the use of proceeds;

(vi) Consistent with safe and sound practices, if the consumer or the consumer's legal representative specifically requests that the creditor use medical information in determining the consumer's eligibility, or continued eligibility, for credit, to accommodate the consumer's particular circumstances, and such request is documented by the creditor;

(vii) Consistent with safe and sound practices, to determine whether the provisions of a forbearance practice or program that is triggered by a medical event or condition apply to a consumer;

(viii) To determine the consumer's eligibility for, the triggering of, or the reactivation of a debt cancellation contract or debt suspension agreement if a medical condition or event is a triggering event for the provision of benefits under the contract or agreement; or

(ix) To determine the consumer's eligibility for, the triggering of, or the reactivation of a credit insurance product if a medical condition or event is a triggering event for the provision of benefits under the product.

(2) *Example of determining eligibility for a special credit program or credit assistance program.* A not-for-profit organization establishes a credit assistance program pursuant to a written plan that is designed to assist disabled veterans in purchasing homes by subsidizing the down payment for the home purchase mortgage loans of qualifying veterans. The organization works through mortgage lenders and requires mortgage lenders to obtain medical information about the disability of any consumer that seeks to qualify for the program, use that information to verify the consumer's eligibility for the program, and forward that information to the organization. A consumer who is a veteran applies to a creditor for a home purchase mortgage loan. The creditor informs the consumer about the credit assistance program for disabled veterans and the consumer seeks to qualify for the program. Assuming that the program complies with all applicable law, including applicable fair lending laws, the creditor may obtain and use medical information about the medical condition and disability, if any, of the consumer to determine whether the consumer qualifies for the credit assistance program.

(3) *Examples of verifying the medical purpose of the loan or the use of proceeds.* (i) If a consumer applies for $10,000 of credit for the purpose of financing vision correction surgery, the creditor may verify with the surgeon that the procedure will be performed. If the surgeon reports that surgery will not be performed on the consumer, the creditor may use that medical information to deny the consumer's application for credit, because the loan would not be used for the stated purpose.

(ii) If a consumer applies for $10,000 of credit for the purpose of financing cosmetic surgery, the creditor may confirm the cost of the procedure with the surgeon. If the surgeon reports that the cost of the procedure is $5,000, the creditor may use that medical information to offer the consumer only $5,000 of credit.

(iii) A creditor has an established medical loan program for financing particular elective surgical procedures. The creditor receives a loan application from a consumer requesting $10,000 of credit under the established loan program for an elective surgical procedure. The consumer indicates on the application that the purpose of the loan is to finance an elective surgical procedure not eligible for funding under the guidelines of the established loan program. The creditor may deny the consumer's application because the purpose of the loan is not for a particular procedure funded by the established loan program.

(4) *Examples of obtaining and using medical information at the request of the consumer.* (i) If a consumer applies for a loan and specifically requests that the creditor consider the consumer's medical disability at the relevant time as an explanation for adverse payment history information in his credit report, the creditor may consider such medical information in evaluating the consumer's willingness and ability to repay the requested loan to accommodate the consumer's particular circumstances, consistent with safe and sound practices. The creditor may also decline to consider such medical information to accommodate the consumer, but may evaluate the consumer's application in accordance with its otherwise applicable underwriting criteria. The creditor may not deny the consumer's application or otherwise treat the consumer less favorably because the consumer specifically requested a medical accommodation, if the creditor would have extended the credit or treated the

consumer more favorably under the creditor's otherwise applicable underwriting criteria.

(ii) If a consumer applies for a loan by telephone and explains that his income has been and will continue to be interrupted on account of a medical condition and that he expects to repay the loan by liquidating assets, the creditor may, but is not required to, evaluate the application using the sale of assets as the primary source of repayment, consistent with safe and sound practices, provided that the creditor documents the consumer's request by recording the oral conversation or making a notation of the request in the consumer's file.

(iii) If a consumer applies for a loan and the application form provides a space where the consumer may provide any other information or special circumstances, whether medical or non-medical, that the consumer would like the creditor to consider in evaluating the consumer's application, the creditor may use medical information provided by the consumer in that space on that application to accommodate the consumer's application for credit, consistent with safe and sound practices, or may disregard that information.

(iv) If a consumer specifically requests that the creditor use medical information in determining the consumer's eligibility, or continued eligibility, for credit and provides the creditor with medical information for that purpose, and the creditor determines that it needs additional information regarding the consumer's circumstances, the creditor may request, obtain, and use additional medical information about the consumer as necessary to verify the information provided by the consumer or to determine whether to make an accommodation for the consumer. The consumer may decline to provide additional information, withdraw the request for an accommodation, and have the application considered under the creditor's otherwise applicable underwriting criteria.

(v) If a consumer completes and signs a credit application that is not for medical purpose credit and the application contains boilerplate language that routinely requests medical information from the consumer or that indicates that by applying for credit the consumer authorizes or consents to the creditor obtaining and using medical information in connection with a determination of the consumer's eligibility, or continued eligibility, for credit, the consumer has not specifically requested that the creditor obtain and use medical information to accommodate the consumer's particular circumstances.

(5) *Example of a forbearance practice or program.* After an appropriate safety and soundness review, a creditor institutes a program that allows consumers who are or will be hospitalized to defer payments as needed for up to three months, without penalty, if the credit account has been open for more than one year and has not previously been in default, and the consumer provides confirming documentation at an appropriate time. A consumer is hospitalized and does not pay her bill for a particular month. This consumer has had a credit account with the creditor for more than one year and has not previously been in default. The creditor attempts to contact the consumer and speaks with the consumer's adult child, who is not the consumer's legal representative. The adult child informs the creditor that the consumer is hospitalized and is unable to pay the bill at that time. The creditor defers payments for up to three months, without penalty, for the hospitalized consumer and sends the consumer a letter confirming this practice and the date on which the next payment will be due.

§ 717.31 Limits on redisclosure of information.

(a) *Scope.* This section applies to Federal credit unions.

(b) *Limits on redisclosure.* If a Federal credit union receives medical information about a consumer from a consumer reporting agency or its affiliate, the person must not disclose that information to any other person, except as necessary to carry out the purpose for which the information was initially disclosed, or as otherwise permitted by statute, regulation, or order.

§ 717.32 Sharing medical information with affiliates.

(a) *Scope.* This section applies to Federal credit unions.

(b) *In general.* The exclusions from the term ''consumer report'' in section 603(d)(2) of the Act that allow the sharing of information with affiliates do not apply if a Federal credit union communicates to an affiliate—

(1) Medical information;

(2) An individualized list or description based on the payment transactions of the consumer for medical products or services; or

(3) An aggregate list of identified consumers based on payment transactions for medical products or services.

(c) *Exceptions.* A Federal credit union may rely on the exclusions from the term ''consumer report'' in section 603(d)(2) of the Act to communicate the information in paragraph (b) to an affiliate—

(1) In connection with the business of insurance or annuities (including the activities described in section 18B of the model Privacy of Consumer Financial and Health Information Regulation issued by the National Association of Insurance Commissioners, as in effect on January 1, 2003);

(2) For any purpose permitted without authorization under the regulations promulgated by the Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA);

(3) For any purpose referred to in section 1179 of HIPAA;

(4) For any purpose described in section 502(e) of the Gramm-Leach-Bliley Act;

(5) In connection with a determination of the consumer's eligibility, or continued eligibility, for credit consistent with § 717.30; or

(6) As otherwise permitted by order of the NCUA.

By order of the Board of Governors of the Federal Reserve System, June 2, 2005.

Jennifer J. Johnson,

Secretary of the Board.

Dated: May 25, 2005.

Julie L. Williams,

Acting Comptroller of the Currency.

Dated at Washington, DC, this 16th day of May, 2005.

By order of the Board of Directors.

Federal Deposit Insurance Corporation.

Robert E. Feldman,

Executive Secretary.

Dated: May 19, 2005.

By the Office of Thrift Supervision.

Richard M. Riccobono,

Acting Director.

By the National Credit Union Administration Board on June 1, 2005.

Mary F. Rupp,

Secretary of the Board.

[FR Doc. 05–11356 Filed 6–9–05; 8:45 am]

BILLING CODE 4810–33–P, 6210–01–P, 6714–10–P, 6720–01–P, 7535–01–P